Security Benchmarks™

A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Microsoft Windows Server 2012

v1.0.0

01-31-2013

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, CIS Microsoft Windows Server 2012 Benchmark v1.0.0, provides prescriptive guidance for establishing a secure configuration posture for CIS Microsoft Windows Server 2012. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Windows Server 2012.

Acknowledgements

The configuration recommendations contained in this document reflect consensus between Microsoft Corporation, The National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS).

At the request of Microsoft and the Center for Internet Security, the National Security Agency Information Assurance Directorate participated in the review of these recommendations and provided comments that were incorporated into the final published version.

We would like to thank our customers, partners and government agencies worldwide for their participation and feedback.

Consensus Guidance

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored
Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1- Domain Controller**

  Items in this profile apply to Domain Controllers intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Member Server**

  Items in this profile apply to Member Servers intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

  Items in this profile also apply to Member Servers that have the following Roles enabled:

  - AD Certificate Services
  - DHCP Server
  - DNS Server
  - File Server
  - Hyper-V
  - Network Policy and Access Services
  - Print Server
  - Remote Access Services
  - Remote Desktop Services
  - Web Server

Recommendations

1 Computer Configuration

1.1 Security Settings

1.1.1 Account Policies

1.1.1.1 Set 'Account lockout threshold' to '5 invalid logon attempt(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of failed logon attempts before a lock occurs. Authorized users can lock themselves out of an account by mistyping their password or by remembering it incorrectly, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password will continuously try to authenticate the user, and because the password it uses to authenticate is incorrect, a lock occurs. To avoid accidental lockout of authorized users, set the account lockout threshold to a high number. The default value for this policy setting is 0 invalid logon attempts, which disables the account lockout feature. Because it is possible for an attacker to use this lockout state as a denial of service (DoS) by triggering a lockout on a large number of accounts, your organization should determine whether to use this policy setting based on identified threats and the risks you want to mitigate. There are two options to consider for this policy setting. - Configure the value for Account lockout threshold to 0 to ensure that accounts will not be locked out. This setting value will prevent a DoS attack that attempts to lock out accounts in your organization. It will also reduce help desk calls, because users will not be able to lock themselves out of their accounts accidentally. However, this setting value will not prevent a brute force attack. The following defenses should also be considered: - A password policy that forces all users to have complex passwords made up of 8 or more characters. - A robust auditing mechanism, which will alert administrators when a series of account lockouts occurs in the environment. For example, the auditing solution should monitor for security event 539, which is a logon failure. This event identifies that there was a lock on the account at the time of the logon attempt. The second

option is: - Configure the value for Account lockout threshold to a value that provides users with the ability to mistype their password several times, but locks out the account if a brute force password attack occurs. This configuration will prevent accidental account lockouts and reduce help desk calls, but will not prevent a DoS attack. The recommended state for this setting is: `5 invalid logon attempt(s)`.

Rationale:

Password attacks can use automated methods to try millions of password combinations for any user account. The effectiveness of such attacks can be almost eliminated if you limit the number of failed logons that can be performed. However, a DoS attack could be performed on a domain that has an account lockout threshold configured. An attacker could programmatically attempt a series of password attacks against all users in the organization. If the number of attempts is greater than the account lockout threshold, the attacker might be able to lock out every account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `5 invalid logon attempt(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Account lockout threshold
```

Impact:

If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting will likely generate a number of additional help desk calls. In fact, locked accounts cause the greatest number of calls to the help desk in many organizations. If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value such as 15 minutes. If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Default Value:

0 invalid logon attempts

References:

1. CCE-23909-5

1.1.1.2 Set 'Account lockout duration' to '15 or more minute(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.
Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer. The recommended state for this setting is: `15 or more minute(s)`.

Rationale:

A denial of service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting to 0, then the account will remain locked out until an administrator unlocks it manually.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `15 or more minute(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Account lockout duration
```

Impact:

Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

Default Value:

Not defined

References:

1. CCE-24768-4

1.1.1.3 Set 'Reset account lockout counter after' to '15 minute(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting. If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: `15 minute(s)`.

Rationale:

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `15 minute(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account
Lockout Policy\Reset account lockout counter after
```

Impact:

If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user's account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

Default Value:

0

References:

1. CCE-24840-1

1.1.1.4 Set 'Minimum password length' to '14 or more character(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can

include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: `14 or more character(s).`

Rationale:

Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `14 or more character(s).`

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password
Policy\Minimum password length
```

Impact:

Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Note:

Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Default Value:

0 characters

References:

1. CCE-25317-9

1.1.1.5 Set 'Enforce password history' to '24 or more password(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: `24 or more password(s).`

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.
If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `24 or more password(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history
```

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Default Value:

24 passwords remembered

References:

1. CCE-24644-7

1.1.1.6 Set 'Password must meet complexity requirements' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords. When this policy is enabled, passwords must meet the following minimum requirements: - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters - Be at least six characters in length - Contain characters from three of the following four categories: - English uppercase characters (A through Z) - English lowercase characters (a through z) - Base 10 digits (0 through 9) - Non-alphabetic characters (for example, !, $, #, %) - A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific. Each additional character in a password increases its complexity

exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack. The recommended state for this setting is: `Enabled`.

Rationale:

Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password
Policy\Password must meet complexity requirements
```

Impact:

If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty. If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments. Also, the use of ALT

key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 01280159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Default Value:

Disabled

References:

1. CCE-25602-4

1.1.1.7 Set 'Store passwords using reversible encryption' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password
Policy\Store passwords using reversible encryption
```

Impact:

If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Default Value:

Disabled

References:

1. CCE-23951-7

1.1.1.8 Set 'Minimum password age' to '1 or more day(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: `1 or more day(s).`

Rationale:

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that

is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `1 or more day(s).`

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password
Policy\Minimum password age
```

Impact:

If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

Default Value:

0 days

References:

1. CCE-24018-4

1.1.1.9 Set 'Maximum password age' to '60 or fewer days' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting defines how long a user can use their password before it expires. Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire. The default value for this policy setting is 42 days.
Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users

having to change their password or forgetting which password is current. The recommended state for this setting is: `60 or fewer days`.

Rationale:

The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `60 fewer days`.

```
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password
Policy\Maximum password age
```

Impact:

If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

Default Value:

42 days

References:

1. CCE-24535-7

1.1.2 Advanced Audit Policy Configuration

1.1.2.1 Set 'Audit Policy: Account Logon: Credential Validation' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon. 4775: An account could not be mapped for logon. 4776: The domain controller attempted to validate the credentials for an account. 4777: The domain controller failed to validate the credentials for an account. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential
Validation
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25088-6

1.1.2.2 Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports events generated by the Kerberos Authentication Server. These events occur on the computer that is authoritative for the credentials. Events for this subcategory include: 4768: A Kerberos authentication ticket (TGT) was requested. 4771: Kerberos pre-authentication failed. 4772: A Kerberos authentication ticket request failed. Refer to the Microsoft Knowledgebase article Description of security events in Windows

Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Kerberos
Authentication Service
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24553-0

1.1.2.3 Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports generated by Kerberos ticket request processes on the domain controller that is authoritative for the domain account. Events for this subcategory include: 4769: A Kerberos service ticket was requested. 4770: A Kerberos service ticket was renewed. 4773: A Kerberos service ticket request failed. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Kerberos
Service Ticket Operations
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25549-7

1.1.2.4 Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the events that occur in response to credentials submitted for a user account logon request that do not relate to credential validation or Kerberos tickets. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when

local accounts are used to log on. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Other Account
Logon Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24509-2

1.1.2.5 Set 'Audit Policy: Account Management: Application Group Management' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of application group management on a computer, such as when an application group is created, changed, or deleted or when a member is added to or removed from an application group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of application group accounts. Events for this subcategory include: 4783: A basic application group was created. 4784: A basic application group was changed. 4785: A member was added to a basic application group. 4786: A member was removed from a basic application group. 4787: A non-member was added to a basic application group. 4788: A non-member was removed from a basic application group. 4789: A basic application group was deleted. 4790: An LDAP query group was created. 4791: A basic application group was changed. 4792: An LDAP query group was deleted. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and

force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Application Group Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24868-2

1.1.2.6 Configure 'Audit Policy: Account Management: Computer Account Management' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include:
4741: A computer account was created.
4742: A computer account was changed.
4743: A computer account was deleted.

- Level 1 - Domain Controller. The recommended state for this setting is: `Success and Failure`.
- Level 1 - Member Server. The recommended state for this setting is: `Success`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Computer Account Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data

storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-23482-3

1.1.2.7 Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include: 4744: A security-disabled local group was created. 4745: A security-disabled local group was changed. 4746: A member was added to a security-disabled local group. 4747: A member was removed from a security-disabled local group. 4748: A security-disabled local group was deleted. 4749: A security-disabled global group was created. 4750: A security-disabled global group was changed. 4751: A member was added to a security-disabled global group. 4752: A member was removed from a security-disabled global group. 4753: A security-disabled global group was deleted. 4759: A security-disabled universal group was created. 4760: A security-disabled universal group was changed. 4761: A member was added to a security-disabled universal group. 4762: A member was removed from a security-disabled universal group. 4763: A security-disabled universal group was deleted. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Distribution Group Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25739-4

1.1.2.8 Set 'Audit Policy: Account Management: Other Account Management Events' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed. 4793: The Password Policy Checking API was called. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Other Account Management Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24588-6

1.1.2.9 Set 'Audit Policy: Account Management: Security Group Management' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created. 4728: A member was added to a security-enabled global group. 4729: A member was removed from a security-enabled global group. 4730: A security-enabled global group was deleted. 4731: A security-enabled local group was created. 4732: A member was added to a security-enabled local group. 4733: A member was removed from a security-enabled local group. 4734: A security-enabled local group was deleted. 4735: A security-enabled local group was changed. 4737: A security-enabled global group was changed. 4754: A security-enabled universal group was created. 4755: A security-enabled universal group was changed. 4756: A member was added to a security-enabled universal group. 4757: A member was removed from a security-enabled universal group. 4758: A security-enabled universal group was deleted. 4764: A group's type was changed. Refer to the Microsoft

Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Policy: Account Management:
Security Group Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-23955-8

1.1.2.10 Set 'Audit Policy: Account Management: User Account Management' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created. 4722: A user account was enabled. 4723: An attempt was made to change an account's password. 4724: An attempt was made to reset an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4765: SID History was added to an account. 4766: An attempt to add SID History to an account failed. 4767: A user account was unlocked. 4780: The ACL was set on accounts which are members of administrators groups. 4781: The name of an account was changed: 4794: An attempt was made to set the Directory Services Restore Mode. 5376: Credential Manager credentials were backed up. 5377: Credential Manager credentials were restored from a backup. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits

setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User Account Management
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-25123-1

1.1.2.11 Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports encrypt or decrypt calls into the data protections application interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information. Events for this subcategory include: 4692: Backup of data protection master key was attempted. 4693: Recovery of data protection master key was attempted. 4694: Protection of auditable protected data was attempted. 4695: Unprotection of auditable protected data was attempted. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: DPAPI
Activity
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25011-8

1.1.2.12 Set 'Audit Policy: Detailed Tracking: Process Creation' to 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created. 4696: A primary token was assigned to process. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could

generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking:
Process Creation
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25461-5

1.1.2.13 Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a process terminates. Events for this subcategory include: 4689: A process has exited. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking:
Process Termination
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data

storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25490-4

1.1.2.14 Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports remote procedure call (RPC) connection events. Events for this subcategory include: 5712: A Remote Procedure Call (RPC) was attempted. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: RPC
Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23502-8

1.1.2.15 Set 'Audit Policy: DS Access: Detailed Directory Service Replication' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports detailed information about the information replicating between domain controllers. These events can be very high in volume. Events for this subcategory include:
4928: An Active Directory replica source naming context was established.
4929 : An Active Directory replica source naming context was removed.
4930 : An Active Directory replica source naming context was modified.

4931 : An Active Directory replica destination naming context was modified.
4934 : Attributes of an Active Directory object were replicated.
4935 : Replication failure begins.
4936 : Replication failure ends.
4937 : A lingering object was removed from a replica.
The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Detailed Directory
Service Replication
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23619-0

1.1.2.16 Set 'Audit Policy: DS Access: Directory Service Access' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to domain controllers. Events for this subcategory include:
4662 : An operation was performed on an object. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service
Access
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23953-3

1.1.2.17 Set 'Audit Policy: DS Access: Directory Service Changes' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers. Events for this subcategory include:
5136 : A directory service object was modified.
5137 : A directory service object was created.

5138 : A directory service object was undeleted.
5139 : A directory service object was moved.

The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service
Changes
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24645-4

1.1.2.18 Set 'Audit Policy: DS Access: Directory Service Replication' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports when replication between two domain controllers begins and ends. Events for this subcategory include:
4932: Synchronization of a replica of an Active Directory naming context has begun.
4933: Synchronization of a replica of an Active Directory naming context has ended.
The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects.
If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service
Replication
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24355-0

1.1.2.19 Set 'Audit Policy: Logon-Logoff: Account Lockout' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include: 4625: An account failed to log on. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer

performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Account Lockout
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-24598-5

1.1.2.20 Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of AuthIP during Extended Mode negotiations. Events for this subcategory include: 4978: During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. 4979: IPsec Main Mode and Extended Mode security associations were established. 4980: IPsec Main Mode and Extended Mode security associations were established. 4981: IPsec Main Mode and Extended Mode security associations were established. 4982: IPsec Main Mode and Extended Mode security associations were established. 4983: An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. 4984: An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: IPsec Extended
Mode
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24404-6

1.1.2.21 Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of Internet Key Exchange (IKE) protocol and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations. Events for this subcategory include: 4646: IKE DoS-prevention mode started. 4650: An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used. 4651: An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication. 4652: An IPsec Main Mode negotiation failed. 4653: An IPsec Main Mode negotiation failed. 4655: An IPsec Main Mode security association ended. 4976: During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. 5049: An IPsec Security Association was deleted. 5453: An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.

Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: IPsec Main Mode
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24584-5

1.1.2.22 Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of IKE protocol and AuthIP during Quick Mode negotiations. 4654: An IPsec Quick Mode negotiation failed. Events for this subcategory include: 4977: During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. 5451: An IPsec Quick Mode security association was established. 5452: An IPsec Quick Mode security association ended. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: IPsec Quick Mode
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23614-1

1.1.2.23 Set 'Audit Policy: Logon-Logoff: Logoff' to 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4634: An account was logged off. 4647: User initiated logoff. Refer to the Microsoft Knowledgebase article

Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-24901-1

1.1.2.24 Set 'Audit Policy: Logon-Logoff: Logon' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4624: An account was successfully logged on. 4625: An account failed to log on. 4648: A logon was attempted using explicit credentials. 4675: SIDs were filtered. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logon
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-23670-3

1.1.2.25 Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock. Auditing this setting will result in a medium or high volume of records on NPS and IAS servers. Events for this subcategory include: Note All the events

in the Network Policy Server subcategory are available only in Windows Vista Service Pack 1 and in Windows Server 2008. 6272: Network Policy Server granted access to a user. 6273: Network Policy Server denied access to a user. 6274: Network Policy Server discarded the request for a user. 6275: Network Policy Server discarded the accounting request for a user. 6276: Network Policy Server quarantined a user. 6277: Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy. 6278: Network Policy Server granted full access to a user because the host met the defined health policy. 6279: Network Policy Server locked the user account due to repeated failed authentication attempts. 6280: Network Policy Server unlocked the user account. 8191: Network Policy Server unlocked the user account. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Network Policy
Server
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success and Failure

References:

1. CCE-25189-2

1.1.2.26 Set 'Audit Policy: Logon-Logoff: Other Logon/Logoff Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5378: The requested credentials delegation was disallowed by policy. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a denial of service (DoS). If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other
Logon/Logoff Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24494-7

1.1.2.27 Set 'Audit Policy: Logon-Logoff: Special Logon' to 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include: 4964 : Special groups have been assigned to a new logon. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Special Logon
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-24187-7

1.1.2.28 Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when applications attempt to generate audit events by using the Windows auditing application programming interfaces (APIs). Events for this subcategory include: 4665: An attempt was made to create an application client context. 4666: An application attempted an operation: 4667: An application client context was deleted. 4668: An application was initialized. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events

are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Application
Generated
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25316-1

1.1.2.29 Set 'Audit Policy: Object Access: Central Access Policy Staging' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit access requests where the permission granted or denied by a proposed policy differs from the current central access policy on an object. If you configure this policy setting, an audit event is generated each time a user accesses an object and the permission granted by the current central access policy on the object differs from that granted by the proposed policy. The resulting audit event will be generated as follows: 1) Success audits, when configured, records access attempts when the current central access policy grants access but the proposed policy denies access. 2) Failure audits when configured records access attempts when: a) The current central access policy does not grant access but the proposed policy grants access. b) A principal requests the maximum access rights they are allowed and the access rights granted by the current central access policy are different than the access rights granted by the proposed policy. Volume: Potentially high on a file server when the proposed policy differs significantly from the current central access policy. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Central Access Policy Staging
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24643-9

1.1.2.30 Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when Certification Services operations are performed. Events for this subcategory include: 4868: The certificate manager denied a pending certificate request. 4869: Certificate Services received a resubmitted certificate request. 4870: Certificate Services revoked a certificate. 4871: Certificate Services received a request to publish the certificate revocation list (CRL). 4872: Certificate Services published the

certificate revocation list (CRL). 4873: A certificate request extension changed. 4874: One or more certificate request attributes changed. 4875: Certificate Services received a request to shut down. 4876: Certificate Services backup started. 4877: Certificate Services backup completed. 4878: Certificate Services restore started. 4879: Certificate Services restore completed. 4880: Certificate Services started. 4881: Certificate Services stopped. 4882 : The security permissions for Certificate Services changed. 4883: Certificate Services retrieved an archived key. 4884: Certificate Services imported a certificate into its database. 4885: The audit filter for Certificate Services changed. 4886: Certificate Services received a certificate request. 4887: Certificate Services approved a certificate request and issued a certificate. 4888: Certificate Services denied a certificate request. 4889: Certificate Services set the status of a certificate request to pending. 4890: The certificate manager settings for Certificate Services changed. 4891: A configuration entry changed in Certificate Services. 4892: A property of Certificate Services changed. 4893: Certificate Services archived a key. 4894: Certificate Services imported and archived a key. 4895: Certificate Services published the CA certificate to Active Directory Domain Services. 4896: One or more rows have been deleted from the certificate database. 4897: Role separation enabled: 4898: Certificate Services loaded a template. 4899: A Certificate Services template was updated. 4900: Certificate Services template security was updated. 5120: OCSP Responder Service Started. 5121: OCSP Responder Service Stopped. 5122: A Configuration entry changed in the OCSP Responder Service. 5123: A configuration entry changed in the OCSP Responder Service. 5124: A security setting was updated on OCSP Responder Service. 5125: A request was submitted to OCSP Responder Service. 5126: Signing Certificate was automatically updated by the OCSP Responder Service. 5127: The OCSP Revocation Provider successfully updated the revocation information. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to

be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Certification
Services
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23129-0

1.1.2.31 Set 'Audit Policy: Object Access: Detailed File Share' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit attempts to access files and folders on a shared folder. The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection established between a client and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access. If you configure this policy setting, an audit event is generated when an attempt is made to access a file or folder on a share. The administrator can specify whether to audit only successes, only failures, or both successes and failures. Note: There are no system access control lists (SACLs) for shared folders. If this policy setting is enabled, access to all shared files and folders on the system is audited. Volume: High on a file server or domain controller because of SYSVOL network access required by Group Policy. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Detailed File
Share
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24791-6

1.1.2.32 Set 'Audit Policy: Object Access: File Share' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a file share is accessed. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a file share object that has a specified system access control list (SACL), effectively enabling auditing to take place. A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information: - The security principal (user, computer, or group) to be audited. - The specific access type to be audited, called an access mask. - A flag to indicate whether to audit failed access events, successful access events, or both. If you configure the Audit object access setting to Success, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to Failure, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL. Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the Write and Append Data auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed. Events for this subcategory include: 5140: A network share object was accessed. Refer to

the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: File Share
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24035-8

1.1.2.33 Set 'Audit Policy: Object Access: File System' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when file system objects are accessed. Only file system objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a file system object that has a specified system access control list (SACL), effectively enabling auditing to take place. A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information: - The security principal (user, computer, or group) to be audited. - The specific access type to be audited, called an access mask. - A flag to indicate whether to audit failed access events, successful access events, or both. If you configure the Audit object access setting to Success, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to Failure, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL. Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the Write and Append Data auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed. Events for this subcategory include: 4664: An attempt was made to create a hard link. 4985: The state of a transaction has changed. 5051: A file was virtualized. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: File System
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24456-6

1.1.2.34 Set 'Audit Policy: Object Access: Filtering Platform Connection' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when connections are allowed or blocked by WFP. These events can be high in volume. Events for this subcategory include: 5031: The Windows Firewall Service blocked an application from accepting incoming connections on the network. 5154: The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections. 5155 : The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections. 5156: The Windows Filtering Platform has allowed a connection. 5157: The Windows Filtering Platform has blocked a connection. 5158: The Windows Filtering Platform has permitted a bind to a local port. 5159: The Windows Filtering Platform has blocked a bind to a local port. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Filtering
Platform Connection
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24714-8

1.1.2.35 Set 'Audit Policy: Object Access: Filtering Platform Packet Drop' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when packets are dropped by Windows Filtering Platform (WFP). These events can be very high in volume. Events for this subcategory include: 5152: The Windows Filtering Platform blocked a packet. 5153: A more restrictive Windows Filtering Platform filter has blocked a packet. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting:

http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Filtering
Platform Packet Drop
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24824-5

1.1.2.36 Set 'Audit Policy: Object Access: Handle Manipulation' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a handle to an object is opened or closed. Only objects with SACLs cause these events to be generated, and only if the attempted handle operation matches the SACL. Handle Manipulation events are only generated for object types where the corresponding Object Access subcategory is enabled, for example File System or Registry. Events for this subcategory include: 4656: A handle to an object was requested. 4658: The handle to an object was closed. 4690: An attempt was made to duplicate a handle to an object. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Handle
Manipulation
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24599-3

1.1.2.37 Set 'Audit Policy: Object Access: Kernel Object' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when kernel objects such as processes and mutexes are accessed. Only kernel objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL. Typically kernel objects are only given SACLs if the AuditBaseObjects or AuditBaseDirectories auditing options are enabled. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting:

http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Kernel Object
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23655-4

1.1.2.38 Set 'Audit Policy: Object Access: Other Object Access Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other object access-related events such as Task Scheduler jobs and COM+ objects. Events for this subcategory include: 4671: An application attempted to access a blocked ordinal through the TBS. 4691: Indirect access to an object was requested. 4698: A scheduled task was created. 4699 : A scheduled task was deleted. 4700 : A scheduled task was enabled. 4701: A scheduled task was disabled. 4702 : A scheduled task was updated. 5888: An object in the COM+ Catalog was modified. 5889: An object was deleted from the COM+ Catalog. 5890: An object was added to the COM+ Catalog. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Other Object
Access Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24236-2

1.1.2.39 Set 'Audit Policy: Object Access: Registry' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when registry objects are accessed. Only registry objects with SACLs cause audit events to be generated, and only when they are accessed in a manner matching their SACL. By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses a registry object that has a specified system access control list (SACL), effectively enabling auditing to take place. A

SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information: - The security principal (user, computer, or group) to be audited. - The specific access type to be audited, called an access mask. - A flag to indicate whether to audit failed access events, successful access events, or both. If you configure the Audit object access setting to Success, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to Failure, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL. Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the Write and Append Data auditing setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed. Events for this subcategory include: 4657 : A registry value was modified. 5039: A registry key was virtualized. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Registry
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23630-7

1.1.2.40 Set 'Audit Policy: Object Access: Removable Storage' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events

are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: Removable
Storage
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-22826-2

1.1.2.41 Set 'Audit Policy: Object Access: SAM' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when SAM objects are accessed. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Policy: Object Access: SAM
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by

all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24439-2

1.1.2.42 Set 'Audit Policy: Policy Change: Audit Policy Change' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed. 4719: System audit policy was changed. 4902: The Per-user audit policy table was created. 4904: An attempt was made to register a security event source. 4905: An attempt was made to unregister a security event source. 4906: The CrashOnAuditFail value has changed. 4907: Auditing settings on object were changed. 4908: Special Groups Logon table modified. 4912: Per User Audit Policy was changed. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could

generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Audit Policy Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-25035-7

1.1.2.43 Set 'Audit Policy: Policy Change: Authentication Policy Change' to 'Success' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in authentication policy. Events for this subcategory include: 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4713: Kerberos policy was changed. 4716: Trusted domain information was modified. 4717: System security access was granted to an account. 4718: System security access was removed from an account. 4739: Domain Policy was changed. 4864: A namespace collision was detected. 4865: A trusted forest information entry was added. 4866: A trusted forest information entry was removed. 4867: A trusted forest information entry was modified. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authentication
Policy Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-25674-3

1.1.2.44 Set 'Audit Policy: Policy Change: Authorization Policy Change' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in authorization policy including permissions (DACL) changes. Events for this subcategory include: 4704: A user right was assigned. 4705: A user right was removed. 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4714: Encrypted data recovery policy was changed. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits

setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authorization
Policy Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24421-0

1.1.2.45 Set 'Audit Policy: Policy Change: Filtering Platform Policy Change' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the addition and removal of objects from WFP, including startup filters. These events can be very high in volume. Events for this subcategory include: 4709: IPsec Services was started. 4710: IPsec Services was disabled. 4711: May contain any one of the following: - PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. - PAStore Engine applied Active Directory storage IPsec policy on the computer. - PAStore Engine applied local registry storage IPsec policy on the computer. - PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. - PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. - PAStore Engine failed to apply local registry storage IPsec policy on the computer. - PAStore Engine failed to apply some rules of the active IPsec policy on the computer. - PAStore Engine failed to load directory storage IPsec policy on the computer. - PAStore Engine loaded directory storage IPsec policy on the computer. - PAStore Engine failed to load local storage IPsec policy on the computer. - PAStore Engine loaded local storage IPsec policy on the computer. - PAStore Engine polled for changes to the active IPsec policy and detected no changes. 4712: IPsec Services encountered a potentially serious failure. 5040: A change has been made to IPsec settings. An Authentication Set was added. 5041: A change has been made to IPsec settings. An Authentication Set was modified. 5042: A change has been made to IPsec settings. An Authentication Set was deleted. 5043: A change has been made to IPsec settings. A Connection Security Rule was added. 5044: A change has been made to IPsec settings. A Connection Security Rule was modified. 5045: A change has been made to IPsec settings. A Connection Security Rule was deleted. 5046: A change has been made to IPsec settings. A Crypto Set was added. 5047: A change has been made to IPsec settings. A Crypto Set was modified. 5048: A change has been made to IPsec settings. A Crypto Set was deleted. 5440: The following callout was present when the Windows Filtering Platform Base Filtering Engine started. 5441: The following filter was present when the Windows Filtering Platform Base Filtering Engine started. 5442: The following provider was present when the Windows Filtering Platform Base Filtering Engine started. 5443: The following provider context was present when the Windows Filtering Platform Base Filtering Engine started. 5444 : The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started. 5446: A Windows Filtering Platform callout has been changed. 5448: A Windows Filtering Platform provider has been changed. 5449: A Windows Filtering Platform provider context has been changed. 5450: A Windows Filtering Platform sub-layer has been changed. 5456: PAStore Engine applied Active Directory storage IPsec policy on the computer. 5457: PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. 5458 : PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. 5459: PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. 5460: PAStore

Engine applied local registry storage IPsec policy on the computer. 5461: PAStore Engine failed to apply local registry storage IPsec policy on the computer. 5462: PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem. 5463: PAStore Engine polled for changes to the active IPsec policy and detected no changes. 5464: PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services. 5465: PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully. 5466: PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied. 5467: PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used. 5468: PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used. 5471: PAStore Engine loaded local storage IPsec policy on the computer. 5472: PAStore Engine failed to load local storage IPsec policy on the computer. 5473: PAStore Engine loaded directory storage IPsec policy on the computer. 5474: PAStore Engine failed to load directory storage IPsec policy on the computer. 5477: PAStore Engine failed to add quick mode filter. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Filtering
Platform Policy Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24965-6

1.1.2.46 Set 'Audit Policy: Policy Change: MPSSVC Rule-Level Policy Change' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in policy rules used by the Microsoft Protection Service (MPSSVC.exe). This service is used by Windows Firewall and by Microsoft OneCare. Events for this subcategory include: 4944: The following policy was active when the Windows Firewall started. 4945: A rule was listed when the Windows Firewall started. 4946: A change has been made to Windows Firewall exception list. A rule was added. 4947: A

change has been made to Windows Firewall exception list. A rule was modified. 4948: A change has been made to Windows Firewall exception list. A rule was deleted. 4949: Windows Firewall settings were restored to the default values. 4950: A Windows Firewall setting has changed. 4951: A rule has been ignored because its major version number was not recognized by Windows Firewall. 4952 : Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced. 4953: A rule has been ignored by Windows Firewall because it could not parse the rule. 4954: Windows Firewall Group Policy settings have changed. The new settings have been applied. 4956: Windows Firewall has changed the active profile. 4957: Windows Firewall did not apply the following rule: 4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer: Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: MPSSVC Rule-
Level Policy Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24259-4

1.1.2.47 Set 'Audit Policy: Policy Change: Other Policy Change Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other types of security policy changes such as configuration of the Trusted Platform Module (TPM) or cryptographic providers. Events for this subcategory include: 4909: The local policy settings for the TBS were changed. 4910: The group policy settings for the TBS were changed. 5063: A cryptographic provider operation was attempted. 5064: A cryptographic context operation was attempted. 5065: A cryptographic context modification was attempted. 5066: A cryptographic function operation was attempted. 5067: A cryptographic function modification was attempted. 5068: A cryptographic function provider operation was attempted. 5069: A cryptographic function property operation was attempted. 5070: A cryptographic function property modification was attempted. 5447: A Windows Filtering Platform filter has been changed. 6144: Security policy in the group policy objects has been applied successfully. 6145: One or more errors occurred while processing security policy in the group policy objects. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting:

http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Other Policy
Change Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25169-4

1.1.2.48 Set 'Audit Policy: Privilege Use: Non Sensitive Privilege Use' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user account or service uses a non-sensitive privilege. A non-sensitive privilege includes the following user rights: Access Credential Manager as a trusted caller, Access this computer from the network, Add workstations to domain, Adjust memory quotas for a process, Allow log on locally, Allow log on through Terminal Services, Bypass traverse checking, Change the system time, Create a pagefile, Create global objects, Create permanent shared objects, Create symbolic links, Deny access this computer from the network, Deny log on as a batch job, Deny log on as a service, Deny log on locally, Deny log on through Terminal Services, Force shutdown from a remote system, Increase a process working set, Increase scheduling priority, Lock pages in memory, Log on as a batch job, Log on as a service, Modify an object label, Perform volume maintenance tasks, Profile single process, Profile system performance, Remove computer from docking station, Shut down the system, and Synchronize directory service data. Auditing this subcategory will create a very high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits

setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Non Sensitive Privilege Use
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23876-6

1.1.2.49 Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory is not used. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Other
Privilege Use Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-23920-2

1.1.2.50 Set 'Audit Policy: Privilege Use: Sensitive Privilege Use' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Sensitive
Privilege Use
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-24691-8

1.1.2.51 Set 'Audit Policy: System: IPsec Driver' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets

are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations. 4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer. 4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay. 4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt. 4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored. 5478: IPsec Services has started successfully. 5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. 5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started. 5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits

setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: IPsec Driver
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25372-4

1.1.2.52 Set 'Audit Policy: System: Other System Events' to 'No Auditing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on other system events. Events for this subcategory include: 5024 : The Windows Firewall Service has started successfully. 5025 : The Windows Firewall Service has been stopped. 5027 : The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy. 5028 : The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy. 5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. 5030: The Windows Firewall Service failed to start. 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. 5033 : The Windows Firewall Driver has started successfully. 5034 : The Windows Firewall Driver has been stopped. 5035 : The Windows Firewall Driver failed to start. 5037 : The Windows Firewall Driver detected critical runtime error. Terminating. 5058: Key file operation. 5059: Key migration operation. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `No Auditing`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No Auditing`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Other System Events
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success and Failure

References:

1. CCE-25187-6

1.1.2.53 Set 'Audit Policy: System: Security State Change' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include: 4608: Windows is starting up. 4609: Windows is shutting down. 4616: The system time was changed. 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Security State Change
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success

References:

1. CCE-25178-5

1.1.2.54 Set 'Audit Policy: System: Security System Extension' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority. 4611: A trusted logon process has been registered with the Local Security Authority. 4614: A notification package has been loaded by the Security Account Manager. 4622: A security package has been loaded by the Local Security Authority. 4697: A service was installed in the system. Refer to the Microsoft Knowledgebase article Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: Security System Extension
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

No auditing

References:

1. CCE-25527-3

1.1.2.55 Set 'Audit Policy: System: System Integrity' to 'Success and Failure' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include: 4612 : Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. 4615 : Invalid use of LPC port. 4618 : A monitored security event pattern has occurred. 4816 : RPC detected an integrity violation while decrypting an incoming message. 5038 : Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error. 5056: A cryptographic self test was performed. 5057: A cryptographic primitive operation failed. 5060: Verification operation failed. 5061: Cryptographic operation. 5062: A kernel-mode cryptographic self test was performed. Refer to the Microsoft Knowledgebase article

Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting: http://support.microsoft.com/default.aspx/kb/947226. The recommended state for this setting is: `Success and Failure`.

Rationale:

If audit settings are not configured, it can be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that events are generated for all activities the Security log will be filled with data and hard to use. Also, you can use a large amount of data storage as well as adversely affect overall computer performance if you configure audit settings for a large number of objects. If failure auditing is used and the Audit: Shut down system immediately if unable to log security audits setting in the Security Options section of Group Policy is enabled, an attacker could generate millions of failure events such as logon failures in order to fill the Security log and force the computer to shut down, creating a Denial of Service. If security logs are allowed to be overwritten, an attacker can overwrite part or all of their activity by generating large numbers of events so that the evidence of their intrusion is overwritten.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Success and Failure`.

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Policy: System: System Integrity
```

Impact:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Default Value:

Success and Failure

References:

1. CCE-25093-6

1.1.3 Security Options

1.1.3.1 Accounts

1.1.3.1.1 Configure 'Accounts: Rename administrator account' (Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The Administrator account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.
The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Default Value:

Administrator

References:

1. CCE-23836-0

1.1.3.1.2 Configure 'Accounts: Rename guest account' (Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.

Rationale:

The Guest account exists on all computers that run the Windows 2000, Windows Server 2003, or Windows XP Professional operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

There should be little impact, because the Guest account is disabled by default.

Default Value:

Guest

References:

1. CCE-23675-2

1.1.3.1.3 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer. The recommended state for this setting is: `Enabled`.

Rationale:

Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Limit local account use of blank passwords to console logon only
```

Impact:

None. This is the default configuration.

Default Value:

Enabled

References:

1. CCE-25589-3

1.1.3.2 Audit

1.1.3.2.1 Configure 'Audit: Audit the access of global system objects' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting creates a default system access control list (SACL) for system objects such as mutexes (mutual exclusive), events, semaphores, and MS-DOS devices, and causes access to these system objects to be audited. If the Audit: Audit the access of global system objects setting is enabled, a very large number of security events could quickly fill the Security event log. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

A globally visible named object, if incorrectly secured, could be acted upon by malicious software that knows the name of the object. For instance, if a synchronization object such

as a mutex had a poorly chosen discretionary access control list (DACL), then malicious software could access that mutex by name and cause the program that created it to malfunction. However, the risk of such an occurrence is very low.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you enable the Audit: Audit the access of global system objects setting, a large number of security events could be generated, especially on busy domain controllers and application servers. Such an occurrence could cause servers to respond slowly and force the Security log to record numerous events of little significance. This policy setting can only be enabled or disabled, and there is no way to choose which events are recorded. Even organizations that have the resources to analyze events that are generated by this policy setting would not likely have the source code or a description of what each named object is used for. Therefore, it is unlikely that many organizations could benefit by enabling this policy setting.

Default Value:

Disabled

References:

1. CCE-24075-4

1.1.3.2.2 Configure 'Audit: Audit the use of Backup and Restore privilege' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to audit the use of all user privileges, including Backup and Restore, when the Audit privilege use setting is in effect. If you enable both policies, an audit event will be generated for every file that is backed up or restored. If the Audit: Audit the use of Backup and Restore privilege setting is enabled, a very large number of security events could quickly fill the Security event log. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

When back up and restore is used it creates a copy of the file system that is identical to the target of the backup. Making regular backups and restore volumes is an important part of a your incident response plan, but a malicious user could use a legitimate backup copy to get access to information or spoof a legitimate network resource to compromise your enterprise.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\fullprivilegeauditing
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you enable this policy setting, a large number of security events could be generated, which could cause servers to respond slowly and force the Security event log to record numerous events of little significance. If you increase the Security log size to reduce the chances of a system shutdown, an excessively large log file may affect system performance.

Default Value:

Disabled

References:

1. CCE-24923-5

1.1.3.2.3 Set 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\scenoapplylegacyauditpolicy
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to
override audit policy category settings
```

Impact:

The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit

policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key. Important Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Default Value:

Not defined

References:

1. CCE-24252-9

1.1.3.2.4 Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason. If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. Therefore, this policy setting is configured to Not Defined for both of the environments that are discussed in this chapter. The recommended state for this setting is: `Disabled`.

Rationale:

If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\crashonauditfail
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Shut down system immediately if unable to log security audits
```

Impact:

If you enable this policy setting, the administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

Default Value:

Disabled

References:

1. CCE-23988-9

1.1.3.3 DCOM

1.1.3.3.1 Configure 'DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or groups might access DCOM application remotely or locally. This setting is used to control the attack surface of the computer for DCOM applications. You can use this policy setting to specify access permissions to all the computers to particular users for DCOM applications in the enterprise. When you specify the users or groups that are to be given permission, the security descriptor field is populated with the Security Descriptor Definition Language representation of those groups and privileges. If the security descriptor is left blank, the policy setting is defined in the template, but it is not enforced. Users and groups can be given explicit Allow or Deny privileges on both local access and remote access. The registry settings that are created as a result of enabling the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting take precedence over (have higher priority) the previous registry settings in this area. RpcSs checks the new registry keys in the Policies section for the computer restrictions, and these registry entries take precedence over the existing registry keys under OLE. This means that previously existing registry settings are no longer effective, and if you make changes to the existing settings, the computer access permissions for any users are not changed. You should take care to correctly configure their list of users and groups. The possible values for this policy setting are: Blank. This represents the local security policy way of deleting the policy enforcement key. This value deletes the policy and then sets it as Not defined state. The Blank value is set by using the ACL editor and emptying the list, and then pressing OK. SDDL. This is the Security Descriptor Definition Language representation of the groups and privileges you specify when you enable this policy. Not Defined. This is the default value. Note If the administrator is denied permission to access DCOM applications due to the changes made to DCOM in SP2, the administrator can use the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting to manage DCOM access to the computer. The administrator can specify which users and groups can access the DCOM application on the computer both locally and remotely by using this setting. This will restore control of the DCOM application to the administrator and users. To do this, open the DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL)

syntax setting, and click Edit Security. Specify the groups you want to include and the computer access permissions for those groups. This defines the setting and sets the appropriate SDDL value. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the Remote Procedure Call System Service (RPCSS), a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table, and provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote access, these interfaces can be called by anyone, including unauthenticated users. As a result, RPCSS can be attacked by malicious users who use remote, unauthenticated computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\windows
NT\DCOM\MachineAccessRestriction
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications or components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific call permissions ACL assigns correct permission to appropriate users. If it does not, you need to change your application-specific permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

Default Value:

Not defined

References:

1. CCE-24640-5

1.1.3.3.2 Configure 'DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or groups might launch or activate DCOM applications remotely or locally. This setting is used to control the attack surface of the computer for DCOM applications. You can use this Group Policy setting to grant access to all the computers to particular users for DCOM application in the enterprise. When you define this setting, and specify the users or groups that are to be given permission, the security descriptor field is populated with the Security Descriptor Definition Language representation of those groups and privileges. If the security descriptor is left blank, the policy setting is defined in the template, but it is not enforced. Users and groups can be given explicit Allow or Deny privileges on local launch, remote launch, local activation, and remote activation. The registry settings that are created as a result of this policy take precedence over the previous registry settings in this area. RpcSs checks the new registry keys in the Policies section for the computer restrictions; these entries take precedence over the existing registry keys under OLE. The possible values for this Group Policy setting are: Blank. This represents the local security policy way of deleting the policy enforcement key. This value deletes the policy and then sets it to Not defined state. The Blank value is set by using the ACL editor and emptying the list, and then pressing OK. SDDL. This is the Security Descriptor Definition Language representation of the groups and privileges you specify when you enable this policy. Not Defined. This is the default value. Note If the administrator is denied access to activate and launch DCOM applications due to the changes made to DCOM in SP2, this policy setting can be used for controlling the DCOM activation and launch to the computer. The administrator can specify which users and groups can launch and activate DCOM applications on the computer both locally and remotely by using the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax policy setting. This restores control of the DCOM application to the administrator and specified users. To do this, open the DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax setting, and

click Edit Security. Specify the groups you want to include and the computer launch permissions for those groups. This defines the setting and sets the appropriate SDDL value. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Many COM applications include some security-specific code (for example, to call CoInitializeSecurity) but use weak settings that often allow unauthenticated access to the process. Administrators cannot override these settings to force stronger security in earlier versions of Windows without modifying the application. An attacker could attempt to exploit weak security in an individual application by attacking it through COM calls. Also, COM infrastructure includes the RPCSS, a system service that runs during computer startup and always runs after that. This service manages activation of COM objects and the running object table and provides helper services to DCOM remoting. It exposes RPC interfaces that can be called remotely. Because some COM servers allow unauthenticated remote component activation

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\windows
NT\DCOM\MachineLaunchRestriction
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Windows operating systems implement default COM ACLs when they are installed. Modifying these ACLs from the default may cause some applications to components that communicate by using DCOM to fail. If you implement a COM server and you override the default security settings, confirm that the application-specific launch permissions ACL assigns activation permission to appropriate users. If it does not, you need to change your application-specific launch permission ACL to provide appropriate users with activation rights so that applications and Windows components that use DCOM do not fail.

Default Value:

Not defined

References:

1. CCE-25572-9

1.1.3.4 Devices

1.1.3.4.1 Configure 'Devices: Allow undock without having to log on' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a portable computer can be undocked if the user does not log on to the system. Enable this policy setting to eliminate a Logon requirement and allow use of an external hardware eject button to undock the computer. If you disable this policy setting, a user must log on and have been assigned the Remove computer from docking station user right to undock the computer. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

If this policy setting is enabled, anyone with physical access to portable computers in docking stations could remove them and possibly tamper with them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\undockwithoutlogon
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users who have docked their computers will have to log on to the local console before they can undock their computers. For computers that do not have docking stations, this policy setting will have no impact.

Default Value:

Enabled

References:

1. CCE-25248-6

1.1.3.4.2 Configure 'Devices: Restrict CD-ROM access to locally logged-on user only' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a CD-ROM is accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable CD-ROM media. When this policy setting is enabled and no one is logged on interactively, the CD-ROM is accessible over the network. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

A remote user could potentially access a mounted CD that contains sensitive information. This risk is small, because CD drives are not automatically made available as shared drives; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateCDRoms
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users who connect to the server over the network will not be able to use any CD drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to the CD drive will fail. For example, the Volume Shadow Copy service attempts to access all CD and floppy disk drives that are present on the computer when it initializes, and if the service cannot access one of these drives, it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail. This policy setting would not be suitable for a computer that serves as a CD jukebox for network users.

Default Value:

Disabled

References:

1. CCE-24607-4

1.1.3.4.3 Configure 'Devices: Restrict floppy access to locally logged-on user only' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether removable floppy media are accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable floppy media. If this policy setting is enabled and no one is logged on interactively, the floppy media is accessible over the network. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

A remote user could potentially access a mounted floppy that contains sensitive information. This risk is small because floppy disk drives are not automatically shared; administrators must deliberately choose to share the drive. However, administrators may wish to deny network users the ability to view data or run applications from removable media on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateFloppies
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users who connect to the server over the network will not be able to use any floppy disk drives that are installed on the server whenever anyone is logged on to the local console of the server. System tools that require access to floppy disk drives will fail. For example, the Volume Shadow Copy service attempts to access all CD-ROM and floppy disk drives present on the computer when it initializes, and if the service cannot access one of these drives it will fail. This condition will cause the Windows Backup tool to fail if volume shadow copies were specified for the backup job. Any non-Microsoft backup products that use volume shadow copies will also fail.

Default Value:

Disabled

References:

1. CCE-23668-7

1.1.3.4.4 Set 'Devices: Allowed to format and eject removable media' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines who is allowed to format and eject removable media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: `Administrators`.

Rationale:

Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Allowed to format and eject removable media
```

Impact:

Only Administrators will be able to format and eject removable media. If users are in the habit of using removable media for file transfers and storage, they will need to be informed of the change in policy.

Default Value:

Administrators

References:

1. CCE-25217-1

1.1.3.4.5 Set 'Devices: Prevent users from installing printer drivers' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

It is feasible for a attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network. To reduce the possibility of such an event, only administrators should be allowed to install printer drivers. However, because laptops are mobile devices, laptop users may occasionally need to install a printer driver from a remote source to continue their work. Therefore, this policy setting should be disabled for laptop users, but always enabled for desktop users. The recommended state for this setting is: `Enabled`.

Rationale:

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only Administrators, not users, to do so on servers, because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Devices: Prevent users from installing printer drivers
```

Impact:

Only users with Administrative, Power User, or Server Operator privileges will be able to install printers on the servers. If this policy setting is enabled but the driver for a network printer already exists on the local computer, users can still add the network printer.

Default Value:

Enabled

References:

1. CCE-25176-9

1.1.3.5 Domain controller

1.1.3.5.1 Set 'Domain controller: Allow server operators to schedule tasks' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.
Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu.
The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain controller: Allow server operators to schedule tasks
```

Impact:

The impact should be small for most organizations. Users (including those in the Server Operators group) will still be able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Default Value:

Not defined

References:

1. CCE-25305-4

1.1.3.5.2 Set 'Domain controller: LDAP server signing requirements' to 'Require signing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. The recommended state for this setting is: `Require signing`.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a

client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\ldapserverintegrity
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Require signing`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements
```

Impact:

Clients that do not support LDAP signing will be unable to run LDAP queries against the domain controllers. All Windows 2000based computers in your organization that are managed from Windows Server 2003based or Windows XPbased computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see article 325465, Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100900). Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Default Value:

Not defined

References:

1. CCE-23587-9

1.1.3.5.3 Set 'Domain controller: Refuse machine account password changes' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.

If it is enabled, this setting does not allow a domain controller to accept any changes to a computer account's password.

Default: This policy is not defined, which means that the system treats it as Disabled. The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting on all domain controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes
```

Impact:

None. This is the default configuration.

Default Value:

Not defined

References:

1. CCE-24692-6

1.1.3.6 Domain member

1.1.3.6.1 Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data must be signed and encrypted. Microsoft recommends to configure the Domain member: Digitally encrypt or sign secure channel data (always) setting to Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticatedâ€”and sensitive information such as passwords are encryptedâ€”but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\requiresignorseal
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)
```

Impact:

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following: â€¢ The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98

clients as members of the domain. Potential impacts can include the following: â€¢ The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

Default Value:

Enabled

References:

1. CCE-24465-7

1.1.3.6.2 Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption. Microsoft recommends to configure the Domain member: Digitally encrypt secure channel data (when possible) setting to Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

When a Windows Server 2003, Windows XP, Windows 2000, or Windows NT computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticatedâ€"and sensitive information such as passwords are encryptedâ€"but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\sealsecurechannel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)
```

Impact:

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

Default Value:

Enabled

References:

1. CCE-24414-5

1.1.3.6.3 Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network. Microsoft recommends to configure the Domain member: Digitally sign secure channel data (when possible) setting to Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticatedâ€”and sensitive information such as passwords are encryptedâ€”but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\signsecurechannel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Digitally sign secure channel data (when possible)
```

Impact:

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following: â€¢ The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. â€¢ The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

Default Value:

Enabled

References:

1. CCE-24812-0

1.1.3.6.4 Set 'Domain member: Disable machine account password changes' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member can periodically change its computer account password. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the Domain Member: Maximum machine account password age setting, which by default is every 30 days. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account. The recommended state for this setting is: `Disabled`.

Rationale:

The default configuration for Windows Server 2003based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\disablepasswo
rdchange
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Disable machine account password changes
```

Impact:

None. This is the default configuration.

Default Value:

Disabled

References:

1. CCE-24243-8

1.1.3.6.5 Set 'Domain member: Maximum machine account password age' to '30 or fewer day(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly or set it to 0 so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: `30 or fewer day(s)`.

Rationale:

In Active Directorybased domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `30 or fewer day(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Maximum machine account password age
```

Impact:

None. This is the default configuration.

Default Value:

30 days

References:

1. CCE-23596-0

1.1.3.6.6 Set 'Domain member: Require strong (Windows 2000 or later) session key' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key. To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000based domains is required, it is recommended that you disable this policy setting. The recommended state for this setting is: `Enabled`.

Rationale:

Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\requirestrongkey
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Require strong (Windows 2000 or later) session key
```

Impact:

Computers that have this policy setting enabled will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, computers that do not support this policy setting will not be able to join domains in which the domain controllers have this policy setting enabled.

Default Value:

Disabled

References:

1. CCE-25198-3

1.1.3.7 Interactive logon

1.1.3.7.1 Configure 'Interactive logon: Display user information when the session is locked' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the account name of the last user to log on to the client computers in your organization can display in each computer's respective Windows logon screen. If you enable this policy setting, intruders cannot collect account names visually from the screens of desktop or laptop computers in your organization. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the

name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLockedUserId
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users will always have to type their user names when they log on to the servers.

Default Value:

Not defined

References:

1. CCE-25018-3

1.1.3.7.2 Configure 'Interactive logon: Message text for users attempting to log on' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to

reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.
Note Any warning that you display should first be approved by your organization's legal and human resources representatives.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoti
ceText
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users will see a message in a dialog box before they can log on to the server console.
Note Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.
Important
If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Default Value:

Not defined

References:

1. CCE-25355-9

1.1.3.7.3 Configure 'Interactive logon: Message title for users attempting to log on' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows text to be specified in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoti
ceCaption
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users will see a message in a dialog box before they can log on to the server console. Note Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.

Important
If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Default Value:

Not defined

References:

1. CCE-24020-0

1.1.3.7.4 Configure 'Interactive logon: Require smart card' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting requires users to log on to a computer with a smart card. Note: This setting applies to Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

It can be difficult to make users choose strong passwords, and even strong passwords are vulnerable to brute-force attacks if an attacker has sufficient time and computing resources.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\scforceoption
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

All users of a computer with this setting enabled will have to use smart cards to log onto the local computer, which means that the organization will need a reliable public key infrastructure (PKI) as well as smart cards and smart card readers for these users. These requirements are significant challenges, because expertise and resources are required to plan for and deploy these technologies. However, Windows Server 2003 includes Certificate Services, a highly advanced service for implementing and managing certificates. When Certificate Services is combined with Windows XP or Windows Vista, features such as automatic user and computer enrollment and renewal become available. For more information about deploying Smart Cards with Windows Vista see the paper "Windows Vista Smart Card Infrastructure" available for download at the Microsoft Web site (http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en).

Default Value:

Disabled

References:

1. CCE-24408-7

1.1.3.7.5 Set 'Interactive logon: Do not display last user name' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: `Enabled`.

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name
```

Impact:

Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

Default Value:

Disabled

References:

1. CCE-24748-6

1.1.3.7.6 Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users must press CTRL+ALT+DEL before they log on. If you enable this policy setting, users can log on without this key combination. If you disable this policy setting, users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information. The recommended state for this setting is: `Disabled`.

Rationale:

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path. An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
```

Impact:

Unless they use a smart card to log on, users will have to simultaneously press three keys before the logon dialog box will display.

Default Value:

Disabled

References:

1. CCE-25803-8

1.1.3.7.7 Set 'Interactive logon: Machine inactivity limit' to '900 or fewer seconds' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: `900 of fewer seconds`.

Rationale:

If a user forgets to lock their computer when they walk away its possible that a passerby will hijack it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `900 or fewer seconds`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
```

Impact:

The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Default Value:

Not defined

References:

1. CCE-23043-3

1.1.3.7.8 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: `4 or fewer logon(s).`

Rationale:

The number that is assigned to this policy setting indicates the number of users whose logon information the servers will cache locally. If the number is set to 10, then the server caches logon information for 10 users. When an eleventh user logs on to the computer, the server overwrites the oldest cached logon session.
Users who access the server console will have their logon credentials cached on that server. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to attempt to determine user passwords.
To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\cachedlogonscount
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `4 or fewer logon(s).`

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Number of previous logons to cache (in case domain
controller is not available)
```

Impact:

Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Default Value:

10 logons

References:

1. CCE-24264-4

1.1.3.7.9 Set 'Interactive logon: Prompt user to change password before expiration' to '14 or more day(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to 14 days to sufficiently warn users when their passwords will expire. The recommended state for this setting is: `14 or more day(s)`.

Rationale:

It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\passwordexpirywarning
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `14 or more day(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Prompt user to change password before expiration
```

Impact:

Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire in 14 or fewer days.

Default Value:

14 days

References:

1. CCE-23704-0

1.1.3.7.10 Set 'Interactive logon: Require Domain Controller authentication to unlock workstation' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. Note: This setting applies to

Windows 2000 computers, but it is not available through the Security Configuration Manager tools on these computers. The recommended state for this setting is: `Disabled`.

Rationale:

By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the accountâ€"such as user rights assignments, account lockout, or the account being disabledâ€"are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ForceUnlockLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Require Domain Controller authentication to unlock
workstation
```

Impact:

When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.

Default Value:

Disabled

References:

1. CCE-25643-8

1.1.3.7.11 Set 'Interactive logon: Smart card removal behavior' to 'Lock Workstation' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: `Lock Workstation`.

Rationale:

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\scremoveoption
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Lock Workstation`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Smart card removal behavior
```

Impact:

If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively

manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Default Value:

No Action

References:

1. CCE-24154-7

1.1.3.7.12 Set 'Interactive logon: Machine account lockout threshold' to 10 or fewer invalid logon attempts (Scored)

Profile Applicability:

- Level 1 - Member Server

Description:

The machine lockout policy is enforced only on those machines that have Bitlocker enabled for protecting OS volumes. Please ensure that appropriate recovery password backup policies are enabled.
This security setting determines the number of failed logon attempts that causes the machine to be locked out. A locked out machine can only be recovered by providing recovery key at console. You can set the value between 1 and 999 failed logon attempts. If you set the value to 0, the machine will never be locked out. Values from 1 to 3 will be interpreted as 4.
Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password protected screen savers counts as failed logon attempts.
The machine lockout policy is enforced only on those machines that have Bitlocker enabled for protecting OS volumes. Please ensure that the appropriate recovery password backup policies are enabled. The recommended state for this setting is: `10 or fewer invalid logon attempts`.

Rationale:

This policy setting determines the number of failed logon attempts before a lock occurs. Authorized users can lock themselves out of the computer by mistyping their password or by remembering it incorrectly, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password will continuously try to authenticate the user, and because the password it uses to authenticate

is incorrect, a lock occurs. To avoid accidental lockout of authorized users, set the account lockout threshold to a high number. The default value for this policy setting is 0 invalid logon attempts, which disables the machine lockout feature. There are two options to consider for this policy setting.

- Configure the value for Machine lockout threshold to 0 to ensure that accounts will not be locked out. This setting value will reduce help desk calls, because users will not be able to lock themselves out of their accounts accidentally. However, this setting value will not prevent a brute force attack. The following defenses should also be considered:
- A password policy that forces all users to have complex passwords made up of 8 or more characters.
- A robust auditing mechanism, which will alert administrators when a series of account lockouts occurs in the environment. For example, the auditing solution should monitor for security event 539, which is a logon failure. This event identifies that there was a lock on the account at the time of the logon attempt.
- The second option is:
- Configure the value for Machine lockout threshold to a value that provides users with the ability to mistype their password several times, but locks out the account if a brute force password attack occurs. This configuration will prevent accidental account lockouts and reduce help desk calls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\MaxDevice
PasswordFailedAttempts
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `10 or fewer invalid logon attempts.`

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Machine account lockout threshold
```

Impact:

Because vulnerabilities can exist when this value is configured as well as when it is not configured, two distinct countermeasures are defined. Any organization should weigh the choice between the two based on their identified threats and the risks that they want to mitigate. The two countermeasure options are:

- Configure the Machine Lockout Threshold setting to 0. This configuration ensures that accounts will not be locked out, and also helps reduce help desk calls because users cannot accidentally lock themselves out of their accounts. Because it will not prevent a brute force attack, this configuration should only be chosen if both of the following criteria are explicitly met:
- The password policy requires all users to have complex passwords of 8 or more characters.
- A robust audit mechanism is in place to alert administrators when a series of failed logons occur in the environment.
- Configure the Machine Lockout Threshold setting to a sufficiently high value to provide users with the ability to accidentally mistype their password several times before the machine is locked, but ensure that a brute force password attack will still lock the account. A good recommendation for such a configuration is 50 invalid logon attempts, which will prevent accidental account lockouts and reduce the number of help desk calls. This option is recommended if your organization does not have complex password requirements and an audit policy that alerts administrators to a series of failed logon attempts.

Default Value:

Not defined

References:

1. CCE-22731-4

1.1.3.8 Microsoft network client

1.1.3.8.1 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later

environments. Note When Windows Vistabased computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Requ
ireSecuritySignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (always)
```

Impact:

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively

affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

Default Value:

Disabled

References:

1. CCE-24969-8

1.1.3.8.2 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing. The implementation of digital signing in Windowsbased networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network client will use signing only if the server with which it communicates accepts digitally signed communication. Microsoft recommends to enable The Microsoft network client: Digitally sign communications (if server agrees) setting. Note Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can

potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Enab
leSecuritySignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (if server agrees)
```

Impact:

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

Default Value:

Enabled

References:

1. CCE-24740-3

1.1.3.8.3 Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disable this policy setting to prevent the SMB redirector from sending plaintext passwords during authentication to third-party SMB servers that do not support password encryption. It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network. The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Enab
lePlainTextPassword
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Send unencrypted password to third-party SMB servers
```

Impact:

Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

Default Value:

Disabled

References:

1. CCE-24751-0

1.1.3.9 Microsoft network server

1.1.3.9.1 Configure 'Microsoft network server: Server SPN target name validation level' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\SMBServer
NameHardeningLevel
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

ll Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

Default Value:

Off

References:

1. CCE-24502-7

1.1.3.9.2 Set 'Microsoft network server: Amount of idle time required before suspending session' to '15 or fewer minute(s)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.
A value of 0 will disconnect an idle session as quickly as possible. The maximum value is 99999, which is 208 days; in effect, this value disables the setting. The recommended state for this setting is: `15 or fewer minute(s)`.

Rationale:

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\autodisco
nnect
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `15 or fewer minute(s)`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Amount of idle time required before suspending
session
```

Impact:

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Default Value:

15 minutes

References:

1. CCE-23897-2

1.1.3.9.3 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\requiresecuritysignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
```

Impact:

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server

performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

Default Value:

Disabled

References:

1. CCE-23716-4

1.1.3.9.4 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled. Note Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows

operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\enablesecuritysignature
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)
```

Impact:

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledgebase Article 950876 for more details: http://support.microsoft.com/default.aspx/kb/950876/.

Default Value:

Disabled

References:

1. CCE-24354-3

1.1.3.9.5 Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service will be forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire. If your organization configures logon hours for users, it makes sense to enable this policy setting. The recommended state for this setting is: `Enabled`.

Rationale:

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\enableforcedlogoff
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire
```

Impact:

If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Default Value:

Enabled

References:

1. CCE-24148-9

1.1.3.10 MSS

1.1.3.10.1 Configure 'MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This entry appears as MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments) in the SCE. This entry, when enabled, permits a server to automatically reboot after a fatal crash. It is enabled by default, which is undesirable on highly secure servers. You can add this registry value to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl\ subkey. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

There is some concern that a computer could get stuck in an endless loop of failures and reboots. However, the alternative to this entry may not be much more appealingâ€”the computer will simply stop running.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\AutoReboot
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

The computer will no longer reboot automatically after a failure.

Default Value:

Enabled

References:

1. CCE-24205-7

1.1.3.10.2 Configure 'MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This entry appears as MSS: (AutoShareServer) Enable Administrative Shares (not recommended except for highly secure environments) in the SCE. For additional information, see the Microsoft Knowledge Base article "How to remove administrative shares in Windows Server 2008" at http://support.microsoft.com/kb/954422/en-us. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Because these built-in administrative shares are well-known and present on most Windows computers, malicious users often target them for brute-force attacks to guess passwords as well as other types of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShare
Server
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you delete these shares you could cause problems for administrators and programs or services that rely on these shares. For example, both Microsoft Systems Management Server (SMS) and Microsoft Operations Manager require administrative shares for correct installation and operation. Also, many third-party network backup applications require administrative shares.

Default Value:

Enabled

References:

1. CCE-24217-2

1.1.3.10.3 Configure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry EnableICMPRedirect was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes in the SCE. Internet Control Message Protocol (ICMP) redirects cause the stack to plumb host routes. These routes override the Open Shortest Path First (OSPF)generated routes. It is recommended to configure this setting to Not Defined for

enterprise environments and to Disabled for high security environments. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Default Value:

Enabled

References:

1. CCE-24977-1

1.1.3.10.4 Configure 'MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry Hidden was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\ registry key. The entry appears as MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) in the SCE. You can configure a computer so that it does not send announcements to browsers on the domain. If you do so, you hide the computer from the Browse list, which means that the computer will stop announcing itself to other computers on the same network. An attacker who knows the name of a computer can more easily gather additional information about the system. You can enable this setting to remove one method that an attacker might use to gather information about computers on the network. Also, this setting can help reduce network traffic when enabled. However, the security benefits of this setting are small because attackers can use alternative methods to identify and locate potential targets. For this reason, Microsoft recommends to configure this setting to Enabled in high security environments, and to configure it to Not Defined in enterprise environments. For additional information, see the Knowledge Base article 321710, "HOW TO: Hide a Windows 2000-Based Computer from the Browser List." Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

An attacker who knows the name of a computer can more easily gather additional information about the computer. If you enable this entry, you remove one method that an attacker might use to gather information about computers on the network. Also, if you enable this entry you can help reduce network traffic. However, the vulnerability is small because attackers can use alternative methods to identify and locate potential targets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

The computer will no longer appear on the Browser list or in Network Neighborhood on other computers on the same network.

Default Value:

Not defined

References:

1. CCE-24074-7

1.1.3.10.5 Configure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry KeepAliveTime was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds (300,000 is recommended) in the SCE. This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Default Value:

Not defined

References:

1. CCE-24310-5

1.1.3.10.6 Configure 'MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry NoDefaultExempt was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC\ registry key. The entry appears as MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic in the SCE. The default exemptions to IPsec policy filters are documented in the online help for the specific operating system. These filters make it possible for Internet Key Exchange (IKE) and the Kerberos authentication protocol to function. The filters also make it possible for the network Quality of Service (QoS) to be signaled (RSVP) when the data traffic is secured by IPsec, and for traffic that IPsec might not secure such as multicast and broadcast traffic. IPsec is increasingly used for basic host-firewall packet filtering, particularly in Internet-exposed scenarios, and the affect of these default exemptions has not been fully understood. Therefore, some IPsec administrators may create IPsec policies that they think are secure, but are not actually secure against inbound attacks that use the default exemptions. For additional information, see the Knowledge Base article 811832, "IPSec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios."

Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

As IPsec is increasingly used for basic host-firewall packet filtering, particularly in Internet-exposed scenarios, the affect of these default exemptions has not been fully understood. Some IPsec administrators may create IPsec policies that they think are secure, but are not actually secure against inbound attacks that use the default exemptions. Attackers could forge network traffic that appears to consist of legitimate IKE, RSVP, or Kerberos protocol packets but direct them to other network services on the host.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

After you enable this entry, security policies that already exist may have to be changed to work correctly. For details, refer to the Microsoft Knowledge Base article "IPSec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios" at http://support.microsoft.com/default.aspx?kbid=811832,which was referenced earlier in this section.

Default Value:

Not defined

References:

1. CCE-24253-7

1.1.3.10.7 Configure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry NoNameReleaseOnDemand was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\ Parameters\ registry key. The entry appears as MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers in the SCE. NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windowsbased systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution. For more information, see the Microsoft Knowledge Base article "MS00-047: NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts" at http://support.microsoft.com/default.aspx?kbid=269239.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnD
emand
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Default Value:

Not defined

References:

1. CCE-23715-6

1.1.3.10.8 Configure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry PerformRouterDiscovery was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) in the SCE. This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

An attacker who has gained control of a computer on the same network segment could configure a computer on the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDis
covery
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you disable this entry, Windows Server 2003 (which supports the IRDP) cannot automatically detect and configure default gateway addresses on the computer.

Default Value:

Enable only if DHCP sends the Perform Router Discovery option

References:

1. CCE-23677-8

1.1.3.10.9 Configure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry TCPMaxDataRetransmissions for IPv6 was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6 \Parameters\ registry key. The entry appears as MSS: (TcpMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default) in the SCE. This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured

round-trip time on the connection. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\TcpMaxDataRetransmissions
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Default Value:

5

References:

1. CCE-25202-3

1.1.3.10.10 Configure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry TCPMaxDataRetransmissions was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip \Parameters\ registry key. The entry appears as MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) in the SCE. This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Default Value:

5

References:

1. CCE-25455-7

1.1.3.10.11 Set 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry AutoAdminLogon was added to the template file in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ registry key. The entry appears as MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) in the Security Configuration Editor. This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see the Knowledge Base article 315231, "How to turn on automatic logon in Windows XP." The recommended state for this setting is: `Disabled`.

Rationale:

If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AutoAdminLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
```

Impact:

None. By default this entry is not enabled.

Default Value:

Not defined

References:

1. CCE-24927-6

1.1.3.10.12 Set 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This entry appears as MSS: (DisableIPSourceRouting) IPv6 source routing protection level (protects against packet spoofing) in the SCE. IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: `Highest protection, source routing is completely disabled`.

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSource
Routing
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Highest protection, source routing is completely disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level
(protects against packet spoofing)
```

Impact:

If you configure this value to 2, all incoming source routed packets will be dropped.

Default Value:

Not defined

References:

1. CCE-24452-5

1.1.3.10.13 Set 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry DisableIPSourceRouting was added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ registry key. The entry appears as MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) in the SCE. IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: `Highest protection, source routing is completely disabled`.

Rationale:

An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceR
outing
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Highest protection, source routing is completely disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (DisableIPSourceRouting) IP source routing protection level (protects
against packet spoofing)
```

Impact:

If you configure this value to 2, all incoming source routed packets will be dropped.

Default Value:

Not defined

References:

1. CCE-24968-0

1.1.3.10.14 Set 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry SafeDllSearchMode was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager\ registry key. The entry appears as MSS: (SafeDllSearchMode) Enable Safe DLL search mode

(recommended) in the SCE. The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: - Search folders specified in the system path first, and then search the current working folder. - Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: `Enabled`.

Rationale:

If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
```

Impact:

Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Default Value:

Not defined

References:

1. CCE-23462-5

1.1.3.10.15 Set 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' to '0' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry ScreenSaverGracePeriod was added to the template file in the HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon\ registry key. The entry appears as MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) in the SCE. Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. This setting is configured to 0 seconds for both of the environments that are discussed in this guide. The recommended state for this setting is: `0`.

Rationale:

The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver
grace period expires (0 recommended)
```

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Default Value:

5 seconds

References:

1. CCE-24993-8

1.1.3.10.16 Set 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' to '0.9 or less' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The registry value entry WarningLevel was added to the template file in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security\ registry key. The entry appears as MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning in the SCE. This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: `0.9 or less`.

Rationale:

If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `0.9 or less`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\MSS: (WarningLevel) Percentage threshold for the security event log at which
the system will generate a warning
```

Impact:

This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

Default Value:

Not defined

References:

1. CCE-25110-8

1.1.3.11 Network access

1.1.3.11.1 Configure 'Network access: Do not allow storage of passwords and credentials for network authentication' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the Stored User Names and Passwords feature may save passwords or credentials for later use when it gains domain authentication. If you enable this policy setting, the Stored User Names and Passwords feature of Windows does not store passwords and credentials. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directorybased domain account.

Default Value:

Disabled

References:

1. CCE-23358-5

1.1.3.11.2 Configure 'Network access: Named Pipes that can be accessed anonymously' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. Note: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

You can restrict access over named pipes such as COMNAP and LOCATOR to help prevent unauthorized access to the network. The default list of named pipes and their purpose is provided in the following list: COMNAP - SNABase named pipe. Systems Network Architecture (SNA) is a collection of network protocols that were originally developed for IBM mainframe computers. COMNODE - SNA Server named pipe. SQL\QUERY - Default named pipe for SQL Server. SPOOLSS - Named pipe for the Print Spooler service. EPMAPPER - End Point Mapper named pipe. LOCATOR - Remote Procedure Call Locator service named pipe. TrkWks - Distributed Link Tracking Client named pipe. TrkSvr - Distributed Link Tracking Server named pipe.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. For example, with Microsoft Commercial Internet System 1.0, the Internet Mail Service runs under the Inetinfo process. Inetinfo starts in the context of the System account. When

Internet Mail Service needs to query the Microsoft SQL Server database, it uses the System account, which uses null credentials to access a SQL pipe on the computer that runs SQL Server. To avoid this problem, refer to the Microsoft Knowledge Base article How to access network files from IIS applications, which is located at http://support.microsoft.com/default.aspx?scid=207671.

Default Value:

None

References:

1. CCE-25466-4

1.1.3.11.3 Configure 'Network access: Shares that can be accessed anonymously' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. Note: It can be very dangerous to add other shares to this Group Policy setting. Any network user can access any shares that are listed, which could exposure or corrupt sensitive data. Note: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

Default Value:

Not defined

References:

1. CCE-25592-7

1.1.3.11.4 Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: `Disabled`.

Rationale:

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it

has been renamed. That person could then use the account name to initiate a password guessing attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Allow anonymous SID/Name translation
```

Impact:

Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003based domains. For example, the following computers may not work: â€¢ Windows NT 4.0based Remote Access Service servers. â€¢ Microsoft SQL Serversâ„¢ that run on Windows NT 3.xbased or Windows NT 4.0based computers. â€¢ Remote Access Service or Microsoft SQL servers that run on Windows 2000based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Default Value:

Disabled

References:

1. CCE-24597-7

1.1.3.11.5 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting is: `Enabled`.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares
```

Impact:

It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Default Value:

Disabled

References:

1. CCE-24774-2

1.1.3.11.6 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections cannot enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: `Enabled`.

Rationale:

An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts
```

Impact:

It will be impossible to establish trusts with Windows NT 4.0based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Default Value:

Enabled

References:

1. CCE-23082-1

1.1.3.11.7 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what additional permissions are assigned for anonymous connections to the computer. If you enable this policy setting, anonymous Windows users are allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks. The recommended state for this setting is: `Disabled`.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Let Everyone permissions apply to anonymous users
```

Impact:

None. This is the default configuration.

Default Value:

Disabled

References:

1. CCE-23807-1

1.1.3.11.8 Set 'Network access: Remotely accessible registry paths and sub-paths' to 'System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Softwar (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths and sub-paths will be accessible when an application or process references the WinReg key to determine access permissions. Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008, and Windows Server 2003 does not exist in Windows XP. Note: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
```

```
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

Rationale:

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPa
ths\Machine
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Remotely accessible registry paths and sub-paths
```

Impact:

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

Default Value:

System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog

References:

1. CCE-25426-8

1.1.3.11.9 Set 'Network access: Remotely accessible registry paths' to 'System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths will be accessible after referencing the WinReg key to determine access permissions to the paths. Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and subpaths" in Windows Server 2003, Windows Vista, and Windows Server 2008. Note: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:

```
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
```

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
```

Impact:

Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

Default Value:

System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion

References:

1. CCE-23899-8

1.1.3.11.10 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccess with the value 1 in the HKLM\System \CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment. The recommended state for this setting is: `Enabled`.

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\restrictn
ullsessaccess
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Restrict anonymous access to Named Pipes and Shares
```

Impact:

You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the Network access: Named pipes that can be accessed anonymously: - COMNAPSNA session access -

COMNODESNA session access - SQL\QUERYSQL instance access - SPOOLSSSpooler service - LLSRPCLicense Logging service - NetlogonNet Logon service - LsarpcLSA access - SamrRemote access to SAM objects - browserComputer Browser service Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Default Value:

Enabled

References:

1. CCE-24564-7

1.1.3.11.11 Set 'Network access: Sharing and security model for local accounts' to 'Classic - local users authenticate as themselves' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource. The recommended state for this setting is: `Classic - local users authenticate as themselves`.

Rationale:

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Classic - local users authenticate as themselves`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Sharing and security model for local accounts
```

Impact:

None. This is the default configuration.

Default Value:

Classic - local users authenticate as themselves

References:

1. CCE-22742-1

1.1.3.12 Network security

1.1.3.12.1 Configure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows 7 and Windows Server 2008 R2 introduce an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. You can also develop or add other SSPs. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the

PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. This policy will be turned off by default on domain joined machines. This would disallow the online identities to be able to authenticate to the domain joined machine in Windows 7. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\pku2u\AllowOnlineID
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7.

Default Value:

Not defined

References:

1. CCE-25299-9

1.1.3.12.2 Configure 'Network Security: Configure encryption types allowed for Kerberos' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller

- Level 1 - Member Server

Description:

This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\
Parameters\SupportedEncryptionTypes
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Default Value:

Not defined

References:

1. CCE-24147-1

1.1.3.12.3 Configure 'Network security: Force logoff when logon hours expire' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting, which determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours, affects the SMB component. If you enable this policy setting, client sessions with the SMB server will be disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

If you disable this policy setting, a user could remain connected to the computer outside of their allotted logon hours.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

When a user's logon time expires, SMB sessions will terminate. The user will be unable to log on to the computer until their next scheduled access time commences.

Default Value:

Disabled

References:

1. CCE-25367-4

1.1.3.12.4 Configure 'Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to create an exception list of remote servers to which clients are allowed to use NTLM authentication if the "Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers" policy setting is configured. The naming format for servers on this exception list is the fully qualified domain name (FQDN) or NetBIOS server name used by the application, listed one per line. To ensure exceptions the name used by all applications needs to be in the list, and to ensure an exception is accurate, the server name should be listed in both naming formats . A single asterisk (*) can be used anywhere in the string as a wildcard character. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\ClientAllowedNTLMServer
s
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you configure this policy setting, you can define a list of remote servers to which clients are allowed to use NTLM authentication. If you do not configure this policy setting, no exceptions will be applied.

Default Value:

Not defined

References:

1. CCE-25046-4

1.1.3.12.5 Configure 'Network Security: Restrict NTLM: Add server exceptions in this domain' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to create an exception list of servers in this domain to which clients are allowed to use NTLM pass-through authentication if the "Network Security: Restrict NTLM: Deny NTLM authentication in this domain" is set. The naming format for servers on this exception list is the fully qualified domain name (FQDN) or NetBIOS server name used by the calling application listed one per line. A single asterisk (*) can be used at the beginning or end of the string as a wildcard character. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DCAllowedNTLM
Servers
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you configure this policy setting, you can define a list of servers in this domain to which clients are allowed to use NTLM authentication. If you do not configure this policy setting, no exceptions will be applied.

Default Value:

Not defined

References:

1. CCE-23483-1

1.1.3.12.6 Configure 'Network Security: Restrict NTLM: Audit Incoming NTLM Traffic' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit incoming NTLM traffic. This policy is supported on at least Windows 7 or Windows Server 2008 R2. Note: Audit events are recorded on this computer in the "Operational" Log located under the Applications and Services Log/Microsoft/Windows/NTLM. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you select "Disable", or do not configure this policy setting, the server will not log events for incoming NTLM traffic. If you select "Enable auditing for domain accounts", the server will log events for NTLM pass-through authentication requests that would be blocked when the "Network Security: Restrict NTLM: Incoming NTLM traffic" policy setting is set to the "Deny all domain accounts" option. If you select "Enable auditing for all accounts", the server will log events for all NTLM authentication requests that would be blocked when the "Network Security: Restrict NTLM: Incoming NTLM traffic" policy setting is set to the "Deny all accounts" option.

Default Value:

Not defined

References:

1. CCE-23338-7

1.1.3.12.7 Configure 'Network Security: Restrict NTLM: Audit NTLM authentication in this domain' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit NTLM authentication in a domain from this domain controller. This policy is supported on at least Windows Server 2008 R2. Note: Audit events are recorded on this computer in the "Operational" Log located under the Applications and

Services Log/Microsoft/Windows/NTLM. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you select "Disable" or do not configure this policy setting, the domain controller will not log events for NTLM authentication in this domain. If you select "Enable for domain accounts to domain servers," the domain controller will log events for NTLM authentication logon attempts for domain accounts to domain servers when NTLM authentication would be denied because "Deny for domain accounts to domain servers" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable for domain accounts," the domain controller will log events for NTLM authentication logon attempts that use domain accounts when NTLM authentication would be denied because "Deny for domain accounts" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable for domain servers" the domain controller will log events for NTLM authentication requests to all servers in the domain when NTLM authentication would be denied because "Deny for domain servers" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting. If you select "Enable all" the domain controller will log events for NTLM pass-through authentication requests from its servers and for its accounts

which would be denied because "Deny all" is selected in the "Network security: Restrict NTLM: NTLM authentication in this domain" policy setting.

Default Value:

Not defined

References:

1. CCE-24238-8

1.1.3.12.8 Configure 'Network Security: Restrict NTLM: Incoming NTLM traffic' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to deny or allow incoming NTLM traffic. This policy is supported on at least Windows 7 or Windows Server 2008 R2. Note: Block events are recorded on this computer in the "Operational" Log located under the Applications and Services Log/Microsoft/Windows/NTLM. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictReceivingNTLMTraffic
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you select "Allow all" or do not configure this policy setting, the server will allow all NTLM authentication requests. If you select "Deny all domain accounts," the server will deny NTLM authentication requests for domain logon and display an NTLM blocked error, but allow local account logon. If you select "Deny all accounts," the server will deny NTLM authentication requests from incoming traffic and display an NTLM blocked error.

Default Value:

Not defined

References:

1. CCE-24393-1

1.1.3.12.9 Configure 'Network Security: Restrict NTLM: NTLM authentication in this domain' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller. This policy does not affect interactive logon to this domain controller. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RestrictNTLMInDomain
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you select "Disabled" or do not configure this policy setting, the domain controller will allow all NTLM pass-through authentication requests within the domain. If you select "Deny for domain accounts to domain servers" the domain controller will deny all NTLM authentication logon attempts to all servers in the domain that are using domain accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny for domain account" the domain controller will deny all NTLM authentication logon attempts from domain accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny for domain servers" the domain controller will deny NTLM authentication requests to all servers in the domain and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting. If you select "Deny all," the domain controller will deny all NTLM pass-through authentication requests from its servers and for its accounts and return an NTLM blocked error unless the server name is on the exception list in the "Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain" policy setting.

Default Value:

Not defined

References:

1. CCE-25645-3

1.1.3.12.10 Configure 'Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to deny or audit outgoing NTLM traffic from this Windows 7 or this Windows Server 2008 R2 computer to any Windows remote server. This policy is supported on at least Windows 7 or Windows Server 2008 R2. Note: Audit and block events are recorded on this computer in the "Operational" Log located under the Applications and Services Log/Microsoft/Windows/NTLM. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

NTLM is a Microsoft-developed authentication protocol that uses a challenge-response mechanism for authentication, in which client computers can prove their identities without sending a password to the server. The protocol employs three types of messages to negotiate the request, challenge the authenticity of the sender, and perform the authentication. Kerberos is a more robust protocol and is the preferred method of authentication when available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraf
fic
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you select "Allow all" or do not configure this policy setting, the client computer can authenticate identities to a remote server by using NTLM authentication. If you select "Audit all," the client computer logs an event for each NTLM authentication request to a

remote server. This allows you to identify those servers receiving NTLM authentication requests from the client computer. If you select "Deny all," the client computer cannot authenticate identities to a remote server by using NTLM authentication. You can use the "Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication" policy setting to define a list of remote servers to which clients are allowed to use NTLM authentication.

Default Value:

Not defined

References:

1. CCE-25095-1

1.1.3.12.11 Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation.
This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: `Enabled`.

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\UseMachineId
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM
```

Impact:

If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.
If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Default Value:

Not defined

References:

1. CCE-25508-3

1.1.3.12.12 Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

Allow NTLM to fall back to NULL session when used with LocalSystem.

The default is TRUE up to Windows Vista and FALSE in Windows 7. The recommended state for this setting is: `Disabled`.

Rationale:

NULL sessions are less secure because by definition they are unauthenticated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\allownullsessionfallback
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback
```

Impact:

Any applications that require NULL sessions for LocalSystem will not work as designed.

Default Value:

Not defined

References:

1. CCE-25531-5

1.1.3.12.13 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT' hash. Note Older operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting. The recommended state for this setting is: `Enabled`.

Rationale:

The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Do not store LAN Manager hash value on next password change
```

Impact:

Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

Default Value:

Enabled

References:

1. CCE-24150-5

1.1.3.12.14 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include

transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: - Join a domain - Authenticate between Active Directory forests - Authenticate to down-level domains - Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP) - Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: - Send LM & NTLM responses - Send LM & NTLM â€" use NTLMv2 session security if negotiated - Send NTLM responses only - Send NTLMv2 responses only - Send NTLMv2 responses only\refuse LM - Send NTLMv2 responses only\refuse LM & NTLM - Not Defined The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: - Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Send LM & NTLM use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication). - Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication). These settings correspond to the levels discussed in other Microsoft documents as follows: - Level 0 Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Level 1 Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Level 2 Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Level 3 Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session

security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. - Level 4 Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2. - Level 5 Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state for this setting is: `Send NTLMv2 response only. Refuse LM & NTLM`.

Rationale:

In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responsesâ€"the weakest form of authentication responseâ€"are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Send NTLMv2 response only. Refuse LM & NTLM`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LAN Manager authentication level
```

Impact:

Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM. Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see article 305379, Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100907).

Default Value:

Send NTLMv2 response only

References:

1. CCE-24650-4

1.1.3.12.15 Set 'Network security: LDAP client signing requirements' to 'Negotiate signing' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests, as follows: - None. The LDAP BIND request is issued with the caller-specified options. - Negotiate signing. If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options. - Require signature. This level is the same as Negotiate signing. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. Note: This policy setting does not have any impact on ldap_simple_bind or ldap_simple_bind_s. No Microsoft LDAP clients that are included with Windows XP Professional use ldap_simple_bind or ldap_simple_bind_s to communicate with a domain controller. The possible values for the Network security: LDAP client signing requirements setting are: - None - Negotiate signing - Require signature - Not Defined The recommended state for this setting is: `Negotiate signing`.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Negotiate signing`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LDAP client signing requirements
```

Impact:

If you configure the server to require LDAP signatures you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts.

Default Value:

Negotiate signing

References:

1. CCE-25245-2

1.1.3.12.16 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are: - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. - Not Defined. The recommended state for this setting is: `Require NTLMv2 session security,Require 128-bit encryption`.

Rationale:

You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Require NTLMv2 session security,Require 128-bit encryption`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) clients
```

Impact:

Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

Default Value:

No minimum

References:

1. CCE-24783-3

1.1.3.12.17 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based

(including secure RPC) servers setting are: - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. - Not Defined. The recommended state for this setting is: `Require NTLMv2 session security,Require 128-bit encryption`.

Rationale:

You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Require NTLMv2 session security,Require 128-bit encryption`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including
secure RPC) servers
```

Impact:

Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use

NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.

Default Value:

No minimum

References:

1. CCE-25264-3

1.1.3.13 Recovery console

1.1.3.13.1 Set 'Recovery console: Allow automatic administrative logon' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The recovery console is a command-line environment that is used to recover from system problems. If you enable this policy setting, the administrator account is automatically logged on to the recovery console when it is invoked during startup. The recommended state for this setting is: `Disabled`.

Rationale:

The Recovery Console can be very useful when you need to troubleshoot and repair computers that do not start. However, it is dangerous to allow automatic logon to the console. Anyone could walk up to the server, disconnect the power to shut it down, restart it, select Recover Console from the Restart menu, and then assume full control of the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\securitylevel
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow automatic administrative logon
```

Impact:

Users will have to enter a user name and password to access the Recovery Console.

Default Value:

Disabled

References:

1. CCE-24470-7

1.1.3.13.2 Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting makes the Recovery Console SET command available, which allows you to set the following recovery console environment variables: - AllowWildCards. Enables wildcard support for some commands (such as the DEL command). - AllowAllPaths. Allows access to all files and folders on the computer. - AllowRemovableMedia. Allows files to be copied to removable media, such as a floppy disk. - NoCopyPrompt. Does not prompt when overwriting an existing file. The recommended state for this setting is: `Disabled`.

Rationale:

An attacker who can cause the system to restart into the Recovery Console could steal sensitive data and leave no audit or access trail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\setcommand
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Recovery console: Allow floppy copy and access to all drives and all folders
```

Impact:

Users who have started a server through the Recovery Console and logged in with the built-in Administrator account will not be able to copy files and folders to a floppy disk.

Default Value:

Disabled

References:

1. CCE-25274-2

1.1.3.14 Shutdown

1.1.3.14.1 Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system. The recommended state for this setting is: `Disabled`.

Rationale:

Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on
```

Impact:

Operators will have to log on to servers to shut them down or restart them.

Default Value:

Disabled

References:

1. CCE-25100-9

1.1.3.14.2 Set 'Shutdown: Clear virtual memory pagefile' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this policy setting is enabled, the system pagefile is cleared each time that the system shuts down properly. If you enable this security setting, the

hibernation file (Hiberfil.sys) is zeroed out when hibernation is disabled on a portable computer system. It will take longer to shut down and restart the computer, and will be especially noticeable on computers with large paging files. The recommended state for this setting is: `Disabled`.

Rationale:

Important information that is kept in real memory may be written periodically to the page file to help Windows Server 2003 handle multitasking functions. An attacker who has physical access to a server that has been shut down could view the contents of the paging file. The attacker could move the system volume into a different computer and then analyze the contents of the paging file. Although this process is time consuming, it could expose data that is cached from random access memory (RAM) to the paging file. Caution An attacker who has physical access to the server could bypass this countermeasure by simply unplugging the server from its power source.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\Shutdown: Clear virtual memory pagefile
```

Impact:

It will take longer to shut down and restart the server, especially on servers with large paging files. For a server with 2 gigabytes (GB) of RAM and a 2-GB paging file, this policy setting could increase the shutdown process by 20 to 30 minutes, or more. For some organizations, this downtime violates their internal service level agreements. Therefore, use caution before you implement this countermeasure in your environment.

Default Value:

Disabled

References:

1. CCE-25120-7

1.1.3.15 System cryptography

1.1.3.15.1 Configure 'System cryptography: Force strong key protection for user keys stored on the computer' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users' private keys (such as their S-MIME keys) require a password to be used. If you configure this policy setting so that users must provide a passwordâ€”distinct from their domain passwordâ€”every time that they use a key, then it will be more difficult for an attacker to access locally stored keys, even an attacker who discovers logon passwords. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

If a users account is compromised or their computer is inadvertently left unsecured the malicious user can use the keys stored for the user to access protected resources. You can configure this policy setting so that users must provide a password that is distinct from their domain password every time they use a key. This configuration makes it more difficult for an attacker to access locally stored user keys, even if the attacker takes control of the user's computer and determines their logon password.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Users will have to enter their password every time they access a key that is stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they will be forced to enter the password for that certificate every time they send a signed e-mail message. For some organizations the overhead that is involved using this configuration may be too high. For end user computers that are used to access sensitive data this setting could be set to "User is prompted when the key is first used," but Microsoft does not recommend enforcing this setting on servers due to the significant impact on manageability. For example, if this setting is configured to "User is prompted when the key is first used" you may not be able to configure Remote Desktop Services to use SSL certificates. More information is available in the Windows PKI blog: http://blogs.technet.com/b/pki/archive/2009/06/17/what-is-a-strong-key-protection-in-windows.aspx.

Default Value:

Disabled

References:

1. CCE-23711-5

1.1.3.15.2 Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Although this policy setting increases security, most public Web sites that are secured with TLS or SSL do not support these algorithms. Client computers that have this policy setting enabled will also be unable to connect to Terminal Services on servers that are not configured to use the FIPS compliant algorithms. Note If you enable this policy setting, computer performance will be slower because the 3DES process is performed on each block of data in the file three times. This policy setting should only be enabled if your organization is required to be FIPS compliant. Important: This setting is recorded in different registry locations depending upon the version of Windows being used. For Windows XP and Windows Server 2003 it is stored at

HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy, with Windows Vista and later versions of Windows it is stored at HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled. This means that you must use Windows XP or Windows Server 2003 to edit group policies and security templates which will be applied to computers running Windows XP or Windows Server 2003. However, when editing group policies or security templates which will be applied to computers running Windows Vista or Windows Server 2008 you must use Windows Vista or Windows Server 2008. The recommended state for this setting is: `Enabled`.

Rationale:

You can enable this policy setting to ensure that the computer will use the most powerful algorithms that are available for digital encryption, hashing and signing. Use of these algorithms will minimize the risk of compromise of digitally encrypted or signed data by an unauthorized user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System cryptography: Use FIPS compliant algorithms for encryption, hashing,
and signing
```

Impact:

Client computers that have this policy setting enabled will be unable to communicate by means of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms will not be able to use servers that require them for network communications. For example, many Apache-based Web servers are not configured to support TLS. If you enable this setting, you also need to configure Internet Explorer to use TLS. This policy setting also affects the encryption level that is used for the Remote Desktop Protocol (RDP). The Remote Desktop Connection tool uses the RDP protocol to communicate with servers that run Terminal Services and client computers that are configured for remote control; RDP connections will fail if both computers are not configured to use the same encryption algorithms. To enable Internet

Explore to use TLS 1. On the Internet Explorer Tools menu, click Internet Options. 2. Click the Advanced tab. 3. Select the Use TLS 1.0 check box. It is also possible to configure this policy setting through Group Policy or by using the Internet Explorer Administrators Kit. Client computers running Windows XP, Windows XP SP1 and Windows XP SP2 that try to connect to a Terminal Services server that has this setting enabled will be unable to communicate with the server until an updated version of the Terminal Services client is installed. This issue could allo affect Remote Assistance and Remote Desktop connections. For more information about the issue and how to resolve it see "Remote Assistance connection to Windows Server 2003 with FIPS encryption does not work" at http://support.microsoft.com/default.aspx?scid=kb;en-us;811770. Microsoft .NET Framework applications such as Microsoft ASP.NET that use use cryptographic algorithms which are not validated by NIST to be FIPS 140 compliant may fail. Use of cryptographic algorithm classes that are not FIPS validated will cause an InvalidOperationException exception to occur. See ""System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows" for more information: http://support.microsoft.com/kb/811833. For more information about the impact of this setting see "FIPS 140 Evaluation" available at: http://technet.microsoft.com/en-us/library/cc750357.aspx.

Default Value:

Disabled

References:

1. CCE-23921-0

1.1.3.16 System objects

1.1.3.16.1 Set 'System objects: Require case insensitivity for non-Windows subsystems' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32' subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX

(POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available. The recommended state for this setting is: `Enabled`.

Rationale:

Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\Kernel\ObCaseInsensitive
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Require case insensitivity for non-Windows subsystems
```

Impact:

All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.

Default Value:

Enabled

References:

1. CCE-24870-8

1.1.3.16.2 Set 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create. The recommended state for this setting is: `Enabled`.

Rationale:

This setting determines the strength of the default DACL for objects. Windows Server 2003 maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions. If you enable this setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Strengthen default permissions of internal system objects
(e.g. Symbolic Links)
```

Impact:

None. This is the default configuration.

Default Value:

Enabled

References:

1. CCE-24633-0

1.1.3.17 System settings

1.1.3.17.1 Configure 'System settings: Optional subsystems' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which subsystems are used to support applications in your environment. Note: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

The POSIX subsystem is an Institute of Electrical and Electronic Engineers (IEEE) standard that defines a set of operating system services. The POSIX subsystem is required if the server supports applications that use that subsystem. The POSIX subsystem introduces a security risk that relates to processes that can potentially persist across logons. If a user starts a process and then logs out, there is a potential that the next user who logs on to the computer could access the previous user's process. This potential is dangerous, because anything the second user does with that process will be performed with the privileges of the first user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\SubSystems\optional
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Applications that rely on the POSIX subsystem will no longer operate. For example, Microsoft Services for Unix (SFU) installs an updated version of the POSIX subsystem that is required, so you would need to reconfigure this setting in a Group Policy for any servers that use SFU.

Default Value:

Posix

References:

1. CCE-24878-1

1.1.3.17.2 Set 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. It enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, you can create a certificate rule that will allow or disallow the execution of Authenticode'-signed software, based on the digital certificate that is associated with the software. For certificate rules to take effect in software restriction policies, you must enable this policy setting. The recommended state for this setting is: `Enabled`.

Rationale:

Software restriction policies help to protect users and computers because they can prevent the execution of unauthorized code, such as viruses and Trojans horses.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
```

Impact:

If you enable certificate rules, software restriction policies check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid. This checking process may negatively affect performance when signed programs start. To disable this feature you can edit the software restriction policies in the desired GPO. On the Trusted Publishers Properties dialog box, clear the Publisher and Timestamp check boxes.

Default Value:

Disabled

References:

1. CCE-24939-1

1.1.3.18 User Account Control

1.1.3.18.1 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are: - Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation. - Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: `Enabled`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways: - If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator. - If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdm
inistratorToken
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Admin Approval Mode for the Built-in Administrator
account
```

Impact:

Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Default Value:

Disabled

References:

1. CCE-24134-9

1.1.3.18.2 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user. - Enabled: UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation prompts. If you do not disable the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting, the prompts appear on the interactive user's desktop instead of the secure desktop. - Disabled: (Default) The secure desktop can be disabled only by the user of the interactive desktop or by disabling the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting. The recommended state for this setting is: `Disabled`.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting allows the administrator to perform operations that require elevated privileges while connected via Remote Assistance. This increases security in that organizations can use UAC even when end user support is provided remotely. However, it also reduces security by adding the risk that an administrator might allow an unprivileged user to share elevated privileges for an application that the adminstrator needs to use during the Remote Desktop session.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableUIA
DesktopToggle
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Allow UIAccess applications to prompt for elevation
without using the secure desktop
```

Impact:

If you enable this setting, ("User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop), requests for elevation are automatically sent to the interactive desktop (not the secure desktop) and also appear on the remote administrator's view of the desktop during a Windows Remote Assistance session, and the remote administrator is able to provide the appropriate credentials for elevation. This setting does not change the behavior of the UAC elevation prompt for administrators.

Default Value:

Disabled

References:

1. CCE-23295-9

1.1.3.18.3 Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent for non-Windows binaries' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of the elevation prompt for administrators. The options are: - Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments. - Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege. - Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. - Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. - Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: `Prompt for consent for non-Windows binaries`.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPr
omptBehaviorAdmin
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Prompt for consent for non-Windows binaries`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Behavior of the elevation prompt for administrators in
Admin Approval Mode
```

Impact:

This policy setting controls the behavior of the elevation prompt for administrators.

Default Value:

Prompt for consent for non-Windows binaries

References:

1. CCE-23877-4

1.1.3.18.4 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Prompt for credentials' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of the elevation prompt for standard users. The options are: - Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls. - Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: `Prompt for credentials`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without

the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPr
omptBehaviorUser
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Prompt for credentials`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Behavior of the elevation prompt for standard users
```

Impact:

Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Default Value:

Prompt for credentials

References:

1. CCE-24519-1

1.1.3.18.5 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of application installation detection for the computer. The options are: - Enabled: (Default for home) When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. - Disabled: (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary. The recommended state for this setting is: `Enabled`.

Rationale:

Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation
```

Impact:

Users will need to provide administrative passwords to be able to install programs.

Default Value:

Enabled

References:

1. CCE-24498-8

1.1.3.18.6 Set 'User Account Control: Only elevate executables that are signed and validated' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enforces public key infrastructure (PKI) signature checks for any interactive applications that request elevation of privilege. Enterprise administrators can control which applications are allowed to run by adding certificates to the Trusted Publishers certificate store on local computers. The options are: - Enabled: Enforces the PKI certification path validation for a given executable file before it is permitted to run. - Disabled: (Default) Does not enforce PKI certification path validation before a given executable file is permitted to run. The recommended state for this setting is: `Disabled`.

Rationale:

Intellectual property, personally identifiable information, and other confidential data are normally manipulated by applications on the computer and require elevated credentials to get access to the information. Users and administrators inherently trust applications used with these information sources and provide their credentials. If one of these applications is replaced by a rogue application that appears identical to the trusted application the confidential data could be compromised and the user's administrative credentials would also be compromised.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ValidateAdminCodeSignatures
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Only elevate executables that are signed and validated
```

Impact:

Enabling this setting requires that you have a PKI infrastructure and that your Enterprise administrators have populated the Trusted Root Store with the certificates for the allowed applications. Some older applications are not signed and will not be able to be used in an environment that is hardened with this setting. You should carefully test your applications in a pre-production environment before implementing this setting. For information about the steps required to test application compatibility, make application compatibility fixes, and sign installer packages to prepare your organization for deployment of Windows Vista User Account Control, see Understanding and Configuring User Account Control in Windows Vista (http://go.microsoft.com/fwlink/?LinkID=79026). Control over the applications that are installed on the desktops and the hardware that is able to join your domain should provide similar protection from the vulnerability addressed by this setting. Additionally, the level of protection provided by this setting is not an assurance that all rogue applications will be found

Default Value:

Disabled

References:

1. CCE-23880-8

1.1.3.18.7 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following: - â€¦\Program Files\, including subfolders - â€¦\Windows\system32\ - â€¦\Program Files (x86)\, including subfolders for 64-bit versions of Windows Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level

regardless of the state of this security setting. The options are: - Enabled: (Default) If an application resides in a secure location in the file system, it runs only with UIAccess integrity. - Disabled: An application runs with UIAccess integrity even if it does not reside in a secure location in the file system. The recommended state for this setting is: `Enabled`.

Rationale:

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities: - To set the foreground window. - To drive any application window using SendInput function. - To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput. - To set journal hooks. - To uses AttachThreadInput to attach a thread to a higher integrity input queue.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations
```

Impact:

If the application that requests UIAccess meets the UIAccess setting requirements, Windows Vista starts the application with the ability to bypass most of the UIPI restrictions. If the application does not meet the security restrictions, the application will be started without UIAccess rights and can interact only with applications at the same or lower privilege level.

Default Value:

Enabled

References:

1. CCE-25471-4

1.1.3.18.8 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer. The options are: - Enabled: (Default) Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode. - Disabled: Admin Approval Mode and all related UAC policy settings are disabled. Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced. The recommended state for this setting is: `Enabled`.

Rationale:

This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Run all administrators in Admin Approval Mode
```

Impact:

Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

Default Value:

Enabled

References:

1. CCE-23653-9

1.1.3.18.9 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop. The options are: - Enabled: (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users. - Disabled: All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used. The recommended state for this setting is: `Enabled`.

Rationale:

Elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malicious software.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security
Options\User Account Control: Switch to the secure desktop when prompting for
elevation
```

Impact:

None. This is the default configuration.

Default Value:

Enabled

References:

1. CCE-23656-2

1.1.3.18.10 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software. The options are: - Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry. - Disabled: Applications that write data to protected locations fail. The recommended state for this setting is: `Enabled`.

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations
```

Impact:

None. This is the default configuration.

Default Value:

Enabled

References:

1. CCE-24231-3

1.1.4 User Rights Assignments

1.1.4.1 Configure 'Deny log on through Remote Desktop Services' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users

who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Default Value:

No one

References:

1. CCE-23273-6

1.1.4.2 Configure 'Log on as a service' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows accounts to launch network services or to register a process as a service running on the system. This user right should be restricted on any computer in a high security environment, but because many applications may require this privilege, it should be carefully evaluated and tested before configuring it in an enterprise environment. On Windows Vistabased computers, no users or groups have this privilege by default. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Log on as a service is a powerful user right because it allows accounts to launch network services or services that run continuously on a computer, even when no one is logged on to the console. The risk is reduced by the fact that only users with administrative privileges can install and configure services. An attacker who has already attained that level of access could configure the service to run with the Local System account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Log on as a service user right to additional accounts that are required by those components. IIS requires that this user right be explicitly granted to the ASPNET user account.

Default Value:

No one

References:

1. CCE-25619-8

1.1.4.3 Set 'Access Credential Manager as a trusted caller' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities. The recommended state for this setting is: `No One`.

Rationale:

If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller
```

Impact:

None, this is the default configuration

Default Value:

No one

References:

1. CCE-25683-4

1.1.4.4 Configure 'Access this computer from the network' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based

protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

- Level 1 - Domain Controller. The recommended state for this setting is: `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`.
- Level 1 - Member Server. The recommended state for this setting is: `Administrators, Authenticated Users`.

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network
```

Impact:

If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefor it is recommended that it is assigned to the Users group.If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Default Value:

Everyone, Administrators, Users, Backup Operators

References:

1. CCE-24938-3

1.1.4.5 Set 'Act as part of the operating system' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. The recommended state for this setting is: `No One`.

Rationale:

The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system
```

Impact:

There should be little or no impact because the Act as part of the operating system user right is rarely needed by any accounts other than the Local System account.

Default Value:

No one

References:

1. CCE-25043-1

1.1.4.6 Set 'Add workstations to domain' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting specifies which users can add computer workstations to a specific domain. For this policy setting to take effect, it must be assigned to the user as part of the Default Domain Controller Policy for the domain. A user who has been assigned this right can add up to 10 workstations to the domain. Users who have been assigned the Create Computer Objects permission for an OU or the Computers container in Active Directory can add an unlimited number of computers to the domain, regardless of whether they have been assigned the Add workstations to a domain user right.
By default, all users in the Authenticated Users group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.
In Windowsbased networks, the term security principal is defined as a user, group, or computer that is automatically assigned a security identifier to control access to resources. In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. However, some organizations may want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage the computers. If users are allowed to add computers to the domain, tracking and management efforts would be hampered. Also, users could perform activities that are more difficult to trace because of their ability to create additional unauthorized domain computers.

The recommended state for this setting is: `Administrators`.

Rationale:

The Add workstations to domain user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could install Windows on his or her computer and then add the computer to the domain. The user would know the password for the local administrator account, and could log on with that account and then add his or her domain account to the local Administrators group.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain
```

Impact:

For organizations that have never allowed users to set up their own computers and add them to the domain, this countermeasure will have no impact. For those that have allowed some or all users to configure their own computers, this countermeasure will force the organization to establish a formal process for these procedures going forward. It will not affect existing computers unless they are removed from and re-added to the domain.

Default Value:

Not defined (Authenticated Users for domain controllers)

References:

1. CCE-23271-0

1.1.4.7 Set 'Adjust memory quotas for a process' to 'Administrators, Local Service, Network Service' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: `Administrators, Local Service, Network Service`.

Rationale:

A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators, Local Service, Network Service`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process
```

Impact:

Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. IIS requires that this privilege be explicitly assigned to the IWAM_<ComputerName>, Network Service, and Service accounts. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Default Value:

LOCAL SERVICE, NETWORK SERVICE, Administrators

References:

1. CCE-25112-4

1.1.4.8 Set 'Allow log on locally' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. The recommended state for this setting is: `Administrators`.

Rationale:

Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally
```

Impact:

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. If you have installed optional components such as ASP.NET or Internet Information Services, you may need to assign Allow log on locally user right to additional accounts that are required by those components. For example, IIS 6 requires that this user right be assigned to the IUSR_<ComputerName> account for certain features; see "Default permissions and user rights for IIS 6.0" for more information: http://support.microsoft.com/?id=812614. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

Default Value:

Administrators, Users, Backup Operators

References:

1. CCE-25228-8

1.1.4.9 Set 'Allow log on through Remote Desktop Services' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the restricted groups feature to ensure that no user accounts are part of the Remote Desktop Users group. Restrict this user right to the Administrators group, and possibly the Remote Desktop Users group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. The recommended state for this setting is: `Administrators`.

Rationale:

Any account with the Allow log on through Terminal Services user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Allow log on through Remote Desktop Services
```

Impact:

Removal of the Allow log on through Terminal Services user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Default Value:

Administrators, Remote Desktop Users

References:

1. CCE-24406-1

1.1.4.10 Set 'Back up files and directories' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: `Administrators`.

Rationale:

Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories
```

Impact:

Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Default Value:

Administrators, Backup Operators

References:

1. CCE-25380-7

1.1.4.11 Configure 'Bypass traverse checking' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users who do not have the Traverse Folder access permission to pass through folders when they browse an object path in the NTFS file system or the registry. This user right does not allow users to list the contents of a folder.

- Level - Domain Controller. The recommended state for this setting is: `Administrators, Authenticated Users, Local Service, Network Service`.
- Level - Member Server. The recommended state for this setting is: `Administrators, Authenticated Users, Backup Operators, Local Service, Network Service`.

Rationale:

The default configuration for the Bypass traverse checking setting is to allow all users, including the Everyone group, to bypass traverse checking. Permissions to files and folders are controlled though appropriate configuration of file system access control lists (ACLs),

as the ability to traverse the folder does not provide any read or write permissions to the user. The only scenario in which the default configuration could lead to a mishap would be if the administrator who configures permissions does not understand how this policy setting works. For example, the administrator might expect that users who are unable to access a folder will be unable to access the contents of any child folders. Such a situation is unlikely, and therefore this vulnerability presents little risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Bypass traverse checking
```

Impact:

The Windows operating systems, as well as many applications, were designed with the expectation that anyone who can legitimately access the computer will have this user right. Therefore, we recommend that you thoroughly test any changes to assignments of the Bypass traverse checking user right before you make such changes to production systems. In particular, IIS requires this user right to be assigned to the Network Service, Local Service, IIS_WPG, IUSR_<ComputerName>, and IWAM_<ComputerName> accounts. (It must also be assigned to the ASPNET account through its membership in the Users group.) We recommend that you leave this policy setting at its default configuration.

Default Value:

Everyone, Administrators, Users, Backup Operators, Local Service, Network Service

References:

1. CCE-25271-8

1.1.4.12 Set 'Change the system time' to 'LOCAL SERVICE, Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers. Note: Discrepancies between the time on the local computer and on the domain controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the domain controllers. The recommended state for this setting is: `LOCAL SERVICE, Administrators`.

Rationale:

Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets. The risk from these types of events is mitigated on most domain controllers, member servers, and end-user computers because the Windows Time service automatically synchronizes time with domain controllers in the following ways: â€¢ All client desktop computers and member servers use the authenticating domain controller as their inbound time partner. â€¢ All domain controllers in a domain nominate the primary domain controller (PDC) emulator operations master as their inbound time partner. â€¢ All PDC emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner. â€¢ The PDC emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server. This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `LOCAL SERVICE, Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time
```

Impact:

There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Default Value:

LOCAL SERVICE, Administrators

References:

1. CCE-24185-1

1.1.4.13 Set 'Change the time zone' to 'LOCAL SERVICE, Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers. The recommended state for this setting is: `LOCAL SERVICE, Administrators`.

Rationale:

Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `LOCAL SERVICE, Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone
```

Impact:

None. This is the default configuration.

Default Value:

LOCAL SERVICE, Administrators

References:

1. CCE-24632-2

1.1.4.14 Set 'Create a pagefile' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer. The recommended state for this setting is: `Administrators`.

Rationale:

Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-23972-3

1.1.4.15 Set 'Create a token object' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data. The recommended state for this setting is: `No One`.

Rationale:

A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right. The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object
```

Impact:

None. This is the default configuration.

Default Value:

No one

References:

1. CCE-23939-2

1.1.4.16 Set 'Create global objects' to 'Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right. Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption. The recommended state for this setting is: `Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE`.

Rationale:

Users who can create global objects could affect Windows services and processes that run under other user or system accounts. This capability could lead to a variety of problems, such as application failure, data corruption and elevation of privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects
```

Impact:

None. This is the default configuration.

Default Value:

Administrators, SERVICE, Local Service, Network Service

References:

1. CCE-23850-1

1.1.4.17 Set 'Create permanent shared objects' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right. The recommended state for this setting is: `No One`.

Rationale:

Users who have the Create permanent shared objects user right could create new shared objects and expose sensitive data to the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects
```

Impact:

None. This is the default configuration.

Default Value:

No one

References:

1. CCE-23723-0

1.1.4.18 Set 'Create symbolic links' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system. Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only Administrators can create symbolic links. The recommended state for this setting is: `Administrators`.

Rationale:

Users who have the Create Symbolic Links user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links
```

Impact:

In most cases there will be no impact because this is the default configuration, however, on Windows Servers with the Hyper-V server role installed this user right should also be granted to the special group "Virtual Machines" otherwise you will not be able to create new virtual machines.

Default Value:

Administrators

References:

1. CCE-24549-8

1.1.4.19 Set 'Debug programs' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it. Note Microsoft released several security updates in October 2003 that used a version of Update.exe that required the administrator to have the Debug programs user right. Administrators who did not have this user right were unable to install these security updates until they reconfigured their user rights. This is not typical

behavior for operating system updates. For more information, see Knowledge Base article 830846: "Windows Product Updates may stop responding or may use most or all the CPU resources." The recommended state for this setting is: `Administrators`.

Rationale:

The Debug programs user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to insert rootkit code. By default, the Debug programs user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Debug programs
```

Impact:

If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the Debug programs user right to a separate Group Policy for that OU. The service account that is used for the cluster service needs the Debug programs privilege; if it does not have it, Windows Clustering will fail. For additional information about how to configure Windows Clustering in conjunction with computer hardening, see article 891597, How to apply more restrictive security settings on a Windows Server 2003based cluster server, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100746). Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool Kill.exe requires this user right for administrators to terminate processes that they did not start. Also, some older versions of Update.exe (which is used to install Windows product updates) require the account that applies the update to have this user right. If you install one of the patches that uses this version of Update.exe, the computer could become unresponsive. For more

information, see article 830846, Windows Product Updates may stop responding or may use most or all the CPU resources, in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=100747).

Default Value:

Administrators

References:

1. CCE-23648-9

1.1.4.20 Set 'Deny access to this computer from the network' to 'Guests' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. The recommended state for this setting is: `Guests`.

Rationale:

Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Guests`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Deny access to this computer from the network
```

Impact:

If you configure the Deny access to this computer from the network user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

Default Value:

Guests

References:

1. CCE-24188-5

1.1.4.21 Set 'Deny log on as a batch job' to 'Guests' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is: `Guests`.

Rationale:

Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Guests`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job
```

Impact:

If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely. For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Default Value:

No one

References:

1. CCE-25215-5

1.1.4.22 Set 'Deny log on as a service' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies.Note: This security setting does not apply to the System, Local Service, or Network Service accounts. The recommended state for this setting is: `No One`.

Rationale:

Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service
```

Impact:

If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Default Value:

No one

References:

1. CCE-23117-5

1.1.4.23 Set 'Deny log on locally' to 'Guests' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies.Important:If you apply this security policy to the

Everyone group, no one will be able to log on locally. The recommended state for this setting is: `Guests`.

Rationale:

Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Guests`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally
```

Impact:

If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Default Value:

Guests

References:

1. CCE-24460-8

1.1.4.24 Configure 'Enable computer and user accounts to be trusted for delegation' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.

- Level 1 - Domain Controller. The recommended state for this setting is: `Administrators`.
- Level 1 - Member Server. The recommended state for this setting is: `No One`.

Rationale:

Misuse of the Enable computer and user accounts to be trusted for delegation user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Enable computer and user accounts to be trusted for delegation
```

Impact:

None. This is the default configuration.

Default Value:

No one

References:

1. CCE-25270-0

1.1.4.25 Set 'Force shutdown from a remote system' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to shut down Windows Vistabased computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right. The recommended state for this setting is: `Administrators`.

Rationale:

Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Force shutdown from a remote system
```

Impact:

If you remove the Force shutdown from a remote system user right from the Server Operator group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Default Value:

Administrators

References:

1. CCE-24734-6

1.1.4.26 Set 'Generate security audits' to 'Local Service, Network Service' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or processes can generate audit records in the Security log. The recommended state for this setting is: `Local Service, Network Service`.

Rationale:

An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Local Service, Network Service`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits
```

Impact:

None. This is the default configuration.

Default Value:

Local Service, Network Service

References:

1. CCE-24048-1

1.1.4.27 Set 'Impersonate a client after authentication' to 'Administrators, SERVICE, Local Service, Network Service' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connectâ€”for example, by remote procedure call (RPC) or named pipesâ€”to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels. Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started. Also, a user can impersonate an access token if any of the following conditions exist: - The access token that is being impersonated is for this user. - The user, in this logon session, logged on to the network with explicit credentials to create the access token. - The requested level is less than Impersonate, such as Anonymous or Identify. An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client. The recommended state for this setting is: `Administrators, SERVICE, Local Service, Network Service`.

Rationale:

An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators, SERVICE, Local Service, Network Service`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication
```

Impact:

In most cases this configuration will have no impact. If you have installed optional components such as ASP.NET or IIS, you may need to assign the Impersonate a client after authentication user right to additional accounts that are required by those components, such as IUSR_<ComputerName>, IIS_WPG, ASP.NET or IWAM_<ComputerName>.

Default Value:

Administrators, SERVICE, Local Service, Network Service

References:

1. CCE-24477-2

1.1.4.28 Set 'Increase a process working set' to 'Administrators, Local Service' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This privilege determines which user accounts can increase or decrease the size of a process's working set. The working set of a process is the set of memory pages currently visible to the process in physical RAM memory. These pages are resident and available for an application to use without triggering a page fault. The minimum and maximum working set sizes affect the virtual memory paging behavior of a process. The recommended state for this setting is: `Administrators, Local Service`.

Rationale:

This right is granted to all users by default. However, increasing the working set size for a process decreases the amount of physical memory available to the rest of the system. It would be possible for malicious code to increase the process working set to a level that could severely degrade system performance and potentially cause a denial of service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators, Local Service`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase a process working set
```

Impact:

Users will be unable to increase the working set for their processes, which could degrade performance.

Default Value:

Users

References:

1. CCE-24162-0

1.1.4.29 Set 'Increase scheduling priority' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools. The recommended state for this setting is: `Administrators`.

Rationale:

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-24911-0

1.1.4.30 Set 'Load and unload device drivers' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista. The recommended state for this setting is: `Administrators`.

Rationale:

Device drivers run as highly privileged code. A user who has the Load and unload device drivers user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers
```

Impact:

If you remove the Load and unload device drivers user right from the Print Operators group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

Default Value:

Administrators

References:

1. CCE-24779-1

1.1.4.31 Set 'Lock pages in memory' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur. The recommended state for this setting is: `No One`.

Rationale:

Users with the Lock pages in memory user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory
```

Impact:

None. This is the default configuration.

Default Value:

No one

References:

1. CCE-23829-5

1.1.4.32 Set 'Log on as a batch job' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in enterprise environments. However, its use should be restricted in high security environments to prevent misuse of system resources or to prevent attackers from using the right to launch malicious code after gaining user level access to a computer.

The recommended state for this setting is: `Administrators`.

Rationale:

The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job
```

Impact:

If you configure the Log on as a batch job setting through domainbased Group Policies, the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the Task Scheduler. If you install optional components such as ASP.NET or IIS, you might need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the IIS_WPG group and the IUSR_<ComputerName>, ASPNET, and IWAM_<ComputerName> accounts. If this user right is not assigned o this group and these accounts, IIS will be unable to run some COM objects that are necessary for proper functionality.

Default Value:

Administrators, Backup Operators, Performance Log Users

References:

1. CCE-23386-6

1.1.4.33 Set 'Manage auditing and security log' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can change the auditing options for files and directories and clear the Security log. The recommended state for this setting is: `Administrators`.

Rationale:

The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-23456-7

1.1.4.34 Set 'Modify an object label' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a

user account can modify the label of an object owned by that user to a lower level without this privilege. The recommended state for this setting is: `No One`.

Rationale:

By modifying the integrity label of an object owned by an other user a malicious user may cause them to execute code at a higher level of privilege than intended.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label
```

Impact:

None, by default the Administrators group has this user right.

Default Value:

None

References:

1. CCE-24682-7

1.1.4.35 Set 'Modify firmware environment values' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would

result in a denial of service condition. The recommended state for this setting is: `Administrators`.

Rationale:

Anyone who is assigned the Modify firmware environment values user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-25533-1

1.1.4.36 Set 'Perform volume maintenance tasks' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition. The recommended state for this setting is: `Administrators`.

Rationale:

A user who is assigned the Perform volume maintenance tasks user right could delete a volume, which could result in the loss of data or a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-25070-4

1.1.4.37 Set 'Profile single process' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this

user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right prevents intruders from gaining additional information that could be used to mount an attack on the system. The recommended state for this setting is: `Administrators`.

Rationale:

The Profile single process user right presents a moderate vulnerability. An attacker with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process
```

Impact:

If you remove the Profile single process user right from the Power Users group or other accounts, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

Default Value:

Administrators

References:

1. CCE-23844-4

1.1.4.38 Set 'Profile system performance' to 'Administrators,NT SERVICE\WdiServiceHost' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer. The recommended state for this setting is: `Administrators,NT SERVICE\WdiServiceHost`.

Rationale:

The Profile system performance user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers may also be able to determine what processes are active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators,NT SERVICE\WdiServiceHost`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance
```

Impact:

None. This is the default configuration.

Default Value:

Administrators,NT SERVICE\WdiServiceHost

References:

1. CCE-23802-2

1.1.4.39 Set 'Remove computer from docking station' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows the user of a portable computer to click Eject PC on the Start menu to undock the computer. The recommended state for this setting is: `Administrators`.

Rationale:

Anyone who has the Remove computer from docking station user right can log on and then remove a portable computer from its docking station. If this setting is not defined, it has the same effect as if everyone was granted this right. However, the value of implementing this countermeasure is reduced by the following factors: â€¢ If attackers can restart the computer, they could remove it from the docking station after the BIOS starts but before the operating system starts. â€¢ This setting does not affect servers, because they typically are not installed in docking stations. â€¢ An attacker could steal the computer and the docking station together.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Remove computer from docking station
```

Impact:

By default, only members of the local Administrator group are granted this right. Other user accounts must be explicitly granted the right as necessary. If your organization's users are not members of the local Administrators groups on their portable computers, they will be unable to remove their own portable computers from their docking stations without

shutting them down first. Therefore, you may want to assign the Remove computer from docking station privilege to the local Users group for portable computers.

Default Value:

Administrators

References:

1. CCE-24550-6

1.1.4.40 Set 'Replace a process level token' to 'Local Service, Network Service' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: `Local Service, Network Service`.

Rationale:

User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Local Service, Network Service`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token
```

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Replace a process level token privilege to additional accounts. For example, IIS requires that the Service, Network Service, and IWAM_<ComputerName> accounts be explicitly granted this user right.

Default Value:

LOCAL SERVICE, NETWORK SERVICE

References:

1. CCE-24555-5

1.1.4.41 Set 'Restore files and directories' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: `Administrators`.

Rationale:

An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer. Note Even if the following countermeasure is configured, an attacker could still restore data to a computer in a

domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories
```

Impact:

If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Default Value:

Administrators, Backup Operators

References:

1. CCE-25518-2

1.1.4.42 Set 'Shut down the system' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: `Administrators`.

Rationale:

The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible SingleMaster Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwordsâ€"the Primary Domain Controller (PDC) Emulator role.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Shut down the system
```

Impact:

The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Default Value:

Administrators, Backup Operators

References:

1. CCE-23500-2

1.1.4.43 Set 'Synchronize directory service data' to 'No One' (Scored)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines which users and groups have the authority to synchronize all directory service data. The recommended state for this setting is: `No One`.

Rationale:

The Synchronize directory service data user right affects domain controllers; only domain controllers should be able to synchronize directory service data. Domain controllers have this user right inherently, because the synchronization process runs in the context of the System account on domain controllers. Attackers who have this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No One`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Synchronize directory service data
```

Impact:

None. This is the default configuration.

Default Value:

Not defined

References:

1. CCE-25408-6

1.1.4.44 Set 'Take ownership of files or other objects' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user. The recommended state for this setting is: `Administrators`.

Rationale:

Any users with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects
```

Impact:

None. This is the default configuration.

Default Value:

Administrators

References:

1. CCE-25585-1

1.1.5 Windows Firewall With Advanced Security

1.1.5.1 Public Profile

1.1.5.1.1 Set 'Inbound connections' to 'Enabled:Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: `Enabled:Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DefaultInboundAction
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Inbound connections\Windows Firewall: Public: Inbound connections
```

Then set the `Inbound connections` option to `Block (default)`.

Impact:

None, this is the default configuration.

Default Value:

Block

References:

1. CCE-24839-3

1.1.5.1.2 Set 'Windows Firewall: Public: Allow unicast response' to 'No' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: `No`.

Rationale:

An attacker could respond to broadcast or multicast message with malicious payloads.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DisableUnicastResponsesToMulticastBroadcast
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Allow unicast response
```

Impact:

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for

unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

Default Value:

Yes

References:

1. CCE-25111-6

1.1.5.1.3 Set 'Windows Firewall: Public: Apply local connection security rules' to 'Yes' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: `Yes`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\AllowLocalIPsecPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Apply local connection security
rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-22773-6

1.1.5.1.4 Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\AllowLoca
lPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Apply local firewall rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-24810-4

1.1.5.1.5 Set 'Windows Firewall: Public: Display a notification' to 'Yes' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note When the Apply local firewall rules setting is configured to No. It is recommended to also configuring the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: `Yes`.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DisableNotifications
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Display a notification
```

Impact:

If you configure this policy setting to Yes, Windows Firewall will display these notifications.

Default Value:

Yes

References:

1. CCE-23900-4

1.1.5.1.6 Set 'Windows Firewall: Public: Firewall state' to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\EnableFir
ewall
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `On (recommended)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Public Profile\Windows Firewall: Public: Firewall state
```

Impact:

None, this is the default configuration.

Default Value:

On

References:

1. CCE-23894-9

1.1.5.1.7 Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules

are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: `Allow (default)`.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\DefaultOutboundAction
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Allow (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Windows Firewall: Public: Outbound connections
```

Impact:

None, this is the default configuration.

Default Value:

Allow

References:

1. CCE-23892-3

1.1.5.2 Private Profile

1.1.5.2.1 Set 'Inbound connections' to 'Enabled:Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: `Enabled:Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Windows Firewall: Private: Inbound connections\Windows
Firewall: Private: Inbound connections
```

Then set the `Inbound connections` option to `Block (default)`.

Impact:

None, this is the default configuration.

Default Value:

Block

References:

1. CCE-23486-4

1.1.5.2.2 Set 'Windows Firewall: Private: Allow unicast response' to 'No' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: No.

Rationale:

An attacker could respond to broadcast or multicast message with malicious payloads.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DisableUnicastResponsesToMulticastBroadcast
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to No.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Allow unicast response
```

Impact:

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

Default Value:

Yes

References:

1. CCE-24624-9

1.1.5.2.3 Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\AllowLocalIPsecPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Apply local connection security rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-24738-7

1.1.5.2.4 Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\AllowLocalPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Private Profile\Windows Firewall: Private: Apply local firewall rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-24663-7

1.1.5.2.5 Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note When the Apply local firewall rules setting is configured to No. It is recommended to also configuring the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: `Yes (default)`.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DisableNotifications
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Display a notification
```

Impact:

If you configure this policy setting to Yes, Windows Firewall will display these notifications.

Default Value:

Yes

References:

1. CCE-24907-8

1.1.5.2.6 Set 'Windows Firewall: Private: Firewall state' to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\EnableFirewall
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `On (recommended)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Firewall state
```

Impact:

None, this is the default configuration.

Default Value:

On

References:

1. CCE-23615-8

1.1.5.2.7 Set 'Windows Firewall: Private: Outbound connections' to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules

are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: `Allow (default)`.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\DefaultOutboundAction
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Allow (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Windows Firewall: Private: Outbound connections
```

Impact:

None, this is the default configuration.

Default Value:

Allow

References:

1. CCE-25607-3

1.1.5.3 Domain Profile

1.1.5.3.1 Set 'Inbound connections' to 'Enabled:Block (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: `Enabled:Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Inbound connections\Windows
Firewall: Domain: Inbound connections
```

Then set the `Inbound connections` option to `Block (default)`.

Impact:

None, this is the default configuration.

Default Value:

Block

References:

1. CCE-24808-8

1.1.5.3.2 Set 'Windows Firewall: Domain: Allow unicast response' to 'No' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This option is useful if you need to control whether this computer receives unicast responses to its outgoing multicast or broadcast messages. The recommended state for this setting is: `No`.

Rationale:

An attacker could respond to broadcast or multicast message with malicious payloads.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DisableUnicastResponsesToMulticastBroadcast
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `No`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Allow unicast response
```

Impact:

If you enable this setting and this computer sends multicast or broadcast messages to other computers, Windows Firewall with Advanced Security waits as long as three seconds for unicast responses from the other computers and then blocks all later responses. If you disable this setting and this computer sends a multicast or broadcast message to other computers, Windows Firewall with Advanced Security blocks the unicast responses sent by those other computers.

Default Value:

Yes

References:

1. CCE-25359-1

1.1.5.3.3 Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalIPsecPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Apply local connection security rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-25534-9

1.1.5.3.4 Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: `Yes (default)`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalPolicyMerge
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Apply local firewall rules
```

Impact:

If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Default Value:

Yes

References:

1. CCE-24639-7

1.1.5.3.5 Set 'Windows Firewall: Domain: Display a notification' to 'Yes (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. Note When the Apply local firewall rules setting is configured to No. It is recommended to also configuring the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: `Yes (default)`.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DisableNo
tifications
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Yes (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with
Advanced Security\Windows Firewall with Advanced Security\Windows Firewall
Properties\Domain Profile\Windows Firewall: Domain: Display a notification
```

Impact:

If you configure this policy setting to Yes, Windows Firewall will display these notifications.

Default Value:

Yes

References:

1. CCE-25213-0

1.1.5.3.6 Set 'Windows Firewall: Domain: Firewall state' to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `On (recommended)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Firewall state
```

Impact:

None, this is the default configuration.

Default Value:

On

References:

1. CCE-25350-0

1.1.5.3.7 Set 'Windows Firewall: Domain: Outbound connections' to 'Allow (default)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: `Allow (default)`.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion,

blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\DefaultOutboundAction
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Allow (default)`.

```
Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Windows Firewall: Domain: Outbound connections
```

Impact:

None, this is the default configuration.

Default Value:

Allow

References:

1. CCE-24936-7

1.2 Administrative Templates

1.2.1 Windows Components

1.2.1.1 AutoPlay Policies

1.2.1.1.1 Set 'Turn off Autoplay on:' to 'Enabled:All drives' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

Note You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: `Enabled:All drives`.

Rationale:

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrive
TypeAutoRun
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\AutoPlay
Policies\Turn off Autoplay\Turn off Autoplay
```

Then set the `Turn off Autoplay on:` option to `All drives`.

Impact:

Users will have to manually launch setup or installation programs that are provided on removable media.

Default Value:

Not configured

References:

1. CCE-23878-2

1.2.1.2 Event Log

1.2.1.2.1 Set 'Security: Maximum Log Size (KB)' to 'Enabled:196608 or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:196608 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Security\MaxSize
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)\Specify the maximum log file size (KB)
```

Then set the `Maximum Log Size (KB)` option to `196608 or greater`.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.
The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.
Ideally, all specifically monitored events should be sent to a server that uses Microsoft Operations Manager (MOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Default Value:

20480 KB

References:

1. CCE-24572-0

1.2.1.2.2 Set 'System: Maximum Log Size (KB)' to 'Enabled:32768 or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes.

If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments.

If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:32768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\System\MaxSize
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\System\Specify the maximum log file size (KB)\Specify the maximum log file
size (KB)
```

Then set the `Maximum Log Size (KB)` option to `32768 or greater`.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.
The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.
Ideally, all specifically monitored events should be sent to a server that uses Microsoft Operations Manager (MOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Default Value:

20480 KB

References:

1. CCE-24411-1

1.2.1.2.3 Set 'Application: Maximum Log Size (KB)' to 'Enabled:32768 or greater' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes.

If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1024 kilobytes) and 2 terabytes (2147483647 kilobytes) in kilobyte increments.

If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: `Enabled:32768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Application\MaxSize
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Application\Specify the maximum log file size (KB)\Specify the maximum log
file size (KB)
```

Then set the `Maximum Log Size (KB)` option to `32768 or greater`.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.
The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.
Ideally, all specifically monitored events should be sent to a server that uses Microsoft Operations Manager (MOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Default Value:

20480 KB

References:

1. CCE-24277-6

1.2.1.2.4 Set 'Security: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Note: Old events may or may not be retained according to the "Backup log automatically when full"Â policy setting. The recommended state for this setting is: `Disabled`.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Security\Retention
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Security\Control Event Log behavior when the log file reaches its maximum size
```

Impact:

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.

If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Default Value:

Disabled

References:

1. CCE-24583-7

1.2.1.2.5 Set 'System: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.
Note: Old events may or may not be retained according to the "Backup log automatically when full"Â policy setting. The recommended state for this setting is: `Disabled`.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\System\Retention
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\System\Control Event Log behavior when the log file reaches its maximum size
```

Impact:

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.

If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Default Value:

Disabled

References:

1. CCE-23782-6

1.2.1.2.6 Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Note: Old events may or may not be retained according to the "Backup log automatically when full"Â policy setting. The recommended state for this setting is: `Disabled`.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Application\Retention
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Event Log
Service\Application\Control Event Log behavior when the log file reaches its maximum
size
```

Impact:

If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost.

If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Default Value:

Disabled

References:

1. CCE-23646-3

1.2.1.3 Terminal Services

1.2.1.3.1 Configure 'Encryption Level' (Not Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services\MinEncryptionLevel
```

Remediation:

Configure the following Group Policy setting in a manner that is consistent with the security and operational requirements of your organization:

Impact:

Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

Default Value:

Not configured

References:

1. CCE-24932-6

1.2.1.4 Windows Installer

1.2.1.4.1 Set 'Always install with elevated privileges' to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Directs Windows Installer to use system permissions when it installs any program on the system.

This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.

If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: `Disabled`.

Rationale:

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Installer\Always install with elevated privileges
```

Impact:

Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

Default Value:

Not configured

References:

1. CCE-23919-4

Appendix: Change History

Date	Version	Changes for this version
01-31-2013	1.0.0	Initial Release