Windows Server 2016 Security Technical Implementation Guide

Current release

Authors	
Owner	
Version Number	001.007
Approved by	
Release Date	2018-10-26
Classification	public
Document ID	Windows_Server_2016_STIG

Document History

Version	Author	Date	Description
001.007		2018-10-26	accepted

Change Log in the Current Version

Table of Contents

Notice

This content has been produced from an import of the

IASE Windows Server 2016 STIG V1R7

SCAP datastream into the Scapolite format.

Please refer to the slide set about Scapolite that has been presented at NIST's SCAP v2 workshop for more information about Scapolite.

The machine-readable information on how to implement the settings is *not* part of the original IASE DISA STIG; the information has been added using the mechanisms described in the slide set about automating implementation that has been presented at NIST's SCAP v2 workshop.

Copyright holder for the contents of the IASE Windows Server 2016 STIG V1R7, is IASE DISA, please refer to DoD CyberExchange Website for information about the STIGs and access to the authoritative versions of the STIGs. This project merely uses the STIG as an example of how SCAP content can be expressed and enriched in Scapolite.

For feedback/questions/discussion please use the mailing list

https://list.nist.gov/scap-dev-authoring

Introduction

Objectives

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

SRG-OS-000480-GPOS-00227

SV-87891

Systems must be maintained at a supported servicing level.

Systems must be maintained at a supported servicing level.

Description

VulnDiscussion

Systems at unsupported servicing levels will not receive security updates for new vulnerabilities, which leave them subject to exploitation. Systems must be maintained at a servicing level supported by the vendor with new security updates.

Documentable

false

F-79683r1 Implementation Example

Update the system to a Version 1607 (Build 14393.xxx) or greater.

Version History

Version ‘r1’: created

WN16-00-000110

SRG-OS-000080-GPOS-00048

SV-87899

Local volumes must use a format that supports NTFS attributes.

Local volumes must use a format that supports NTFS attributes.

Description

VulnDiscussion

The ability to set access permissions and auditing is critical to maintaining the security and proper access controls of a system. To support this, volumes must be formatted using a file system that supports NTFS attributes.

Documentable

false

F-79691r1 Implementation Example

Format volumes to use NTFS or ReFS.

Version History

Version ‘r1’: created

WN16-00-000150

SRG-OS-000480-GPOS-00227

SV-87923

Software certificate installation files must be removed from Windows Server 2016.

Software certificate installation files must be removed from Windows Server 2016.

Description

VulnDiscussion

Use of software certificates and their accompanying installation files for end users to access resources is less secure than the use of hardware-based certificates.

Documentable

false

F-79715r1 Implementation Example

Remove any certificate installation files (*.p12 and* .pfx) found on a system.

This does not apply to server-based applications that have a requirement for certificate files.

Version History

Version ‘r1’: created

WN16-00-000270

SRG-OS-000095-GPOS-00049

SV-87939

The Fax Server role must not be installed.

The Fax Server role must not be installed.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Documentable

false

F-79731r1 Implementation Example

Uninstall the “Fax Server” role.

Start “Server Manager”.

Select the server with the role.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “Fax Server” on the “Roles” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000350

SRG-OS-000096-GPOS-00050

SV-87941

The Microsoft FTP service must not be installed unless required.

The Microsoft FTP service must not be installed unless required.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption.

Documentable

false

F-79733r1 Implementation Example

Uninstall the “FTP Server” role.

Start “Server Manager”.

Select the server with the role.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “FTP Server” under “Web Server (IIS)” on the “Roles” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000360

SRG-OS-000095-GPOS-00049

SV-87943

The Peer Name Resolution Protocol must not be installed.

The Peer Name Resolution Protocol must not be installed.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Documentable

false

F-80269r1 Implementation Example

Uninstall the “Peer Name Resolution Protocol” feature.

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “Peer Name Resolution Protocol” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000370

SRG-OS-000095-GPOS-00049

SV-87945

Simple TCP/IP Services must not be installed.

Simple TCP/IP Services must not be installed.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Documentable

false

F-79735r1 Implementation Example

Uninstall the “Simple TCP/IP Services” feature.

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “Simple TCP/IP Services” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000380

SRG-OS-000096-GPOS-00050

SV-87947

The Telnet Client must not be installed.

The Telnet Client must not be installed.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Documentable

false

F-79737r1 Implementation Example

Uninstall the “Telnet Client” feature.

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “Telnet Client” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000390

SRG-OS-000095-GPOS-00049

SV-87949

The TFTP Client must not be installed.

The TFTP Client must not be installed.

Description

VulnDiscussion

Unnecessary services increase the attack surface of a system. Some of these services may not support required levels of authentication or encryption or may provide unauthorized access to the system.

Documentable

false

F-79739r1 Implementation Example

Uninstall the “TFTP Client” feature.

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “TFTP Client” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000400

SRG-OS-000095-GPOS-00049

SV-87951

The Server Message Block (SMB) v1 protocol must be uninstalled.

The Server Message Block (SMB) v1 protocol must be uninstalled.

Description

VulnDiscussion

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks and is not FIPS compliant.

Documentable

false

F-84915r1 Implementation Example

Uninstall the SMBv1 protocol.

Open “Windows PowerShell” with elevated privileges (run as administrator).

Enter “Uninstall-WindowsFeature -Name FS-SMB1 -Restart”. (Omit the Restart parameter if an immediate restart of the system cannot be done.)

Alternately:

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “SMB 1.0/CIFS File Sharing Support” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r2’: created

WN16-00-000410

SRG-OS-000095-GPOS-00049

SV-87953

Windows PowerShell 2.0 must not be installed.

Windows PowerShell 2.0 must not be installed.

Description

VulnDiscussion

Windows PowerShell 5.0 added advanced logging features that can provide additional detail when malware has been run on a system. Disabling the Windows PowerShell 2.0 mitigates against a downgrade attack that evades the Windows PowerShell 5.0 script block logging feature.

Documentable

false

F-79743r1 Implementation Example

Uninstall the “Windows PowerShell 2.0 Engine”.

Start “Server Manager”.

Select the server with the feature.

Scroll down to “ROLES AND FEATURES” in the right pane.

Select “Remove Roles and Features” from the drop-down “TASKS” list.

Select the appropriate server on the “Server Selection” page and click “Next”.

Deselect “Windows PowerShell 2.0 Engine” under “Windows PowerShell” on the “Features” page.

Click “Next” and “Remove” as prompted.

Version History

Version ‘r1’: created

WN16-00-000420

SRG-OS-000329-GPOS-00128

SV-87961

Windows 2016 account lockout duration must be configured to 15 minutes or greater.

Windows 2016 account lockout duration must be configured to 15 minutes or greater.

Description

VulnDiscussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts.

Documentable

false

F-80983r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> “Account lockout duration” to “15” minutes or greater.

A value of “0” is also acceptable, requiring an administrator to unlock the account.

F-80983r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Account Lockout Policy\Account lockout duration
value: 15
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: LockoutDuration
section: System Access
value: 15
```

Version History

Version ‘r2’: created

WN16-AC-000010

SRG-OS-000021-GPOS-00005

SV-87963

The number of allowed bad logon attempts must be configured to three or less.

The number of allowed bad logon attempts must be configured to three or less.

Description

VulnDiscussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. The higher this value is, the less effective the account lockout feature will be in protecting the local system. The number of bad logon attempts must be reasonably small to minimize the possibility of a successful password attack while allowing for honest errors made during normal user logon.

Documentable

false

F-79753r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> “Account lockout threshold” to “3” or fewer invalid logon attempts (excluding “0”, which is unacceptable).

F-79753r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Account Lockout Policy\Account lockout threshold
value: 3
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: LockoutBadCount
section: System Access
value: 3
```

Version History

Version ‘r1’: created

WN16-AC-000020

SRG-OS-000021-GPOS-00005

SV-87965

The period of time before the bad logon counter is reset must be configured to 15 minutes or greater.

The period of time before the bad logon counter is reset must be configured to 15 minutes or greater.

Description

VulnDiscussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that must pass after failed logon attempts before the counter is reset to “0”. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Documentable

false

F-79755r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> “Reset account lockout counter after” to at least “15” minutes.

F-79755r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Account Lockout Policy\Reset account lockout counter after
value: '15'
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: ResetLockoutCount
section: System Access
value: 15
```

Version History

Version ‘r1’: created

WN16-AC-000030

SRG-OS-000077-GPOS-00045

SV-87967

The password history must be configured to 24 passwords remembered.

The password history must be configured to 24 passwords remembered.

Description

VulnDiscussion

A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change to a unique password on a regularly scheduled basis. This enables users to effectively negate the purpose of mandating periodic password changes. The default value is “24” for Windows domain systems. DoD has decided this is the appropriate value for all Windows systems.

Documentable

false

F-79757r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Enforce password history” to “24” passwords remembered.

F-79757r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Password Policy\Enforce password history
value: '24'
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: PasswordHistorySize
section: System Access
value: 24
```

Version History

Version ‘r1’: created

WN16-AC-000040

SRG-OS-000076-GPOS-00044

SV-87969

The maximum password age must be configured to 60 days or less.

The maximum password age must be configured to 60 days or less.

Description

VulnDiscussion

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the passwords. Scheduled changing of passwords hinders the ability of unauthorized system users to crack passwords and gain access to a system.

Documentable

false

F-79759r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Maximum password age” to “60” days or less (excluding “0”, which is unacceptable).

F-79759r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Password Policy\Maximum password age
value: 60
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MaximumPasswordAge
section: System Access
value: 60
```

Version History

Version ‘r1’: created

WN16-AC-000050

SRG-OS-000075-GPOS-00043

SV-87971

The minimum password age must be configured to at least one day.

The minimum password age must be configured to at least one day.

Description

VulnDiscussion

Permitting passwords to be changed in immediate succession within the same day allows users to cycle passwords through their history database. This enables users to effectively negate the purpose of mandating periodic password changes.

Documentable

false

F-79761r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Minimum password age” to at least “1” day.

F-79761r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Password Policy\Minimum password age
value: '1'
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MinimumPasswordAge
section: System Access
value: 1
```

Version History

Version ‘r1’: created

WN16-AC-000060

SRG-OS-000078-GPOS-00046

SV-87973

The minimum password length must be configured to 14 characters.

The minimum password length must be configured to 14 characters.

Description

VulnDiscussion

Information systems not protected with strong password schemes (including passwords of minimum length) provide the opportunity for anyone to crack the password, thus gaining access to the system and compromising the device, information, or the local network.

Documentable

false

F-79763r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Minimum password length” to “14” characters.

F-79763r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Password Policy\Minimum password length
value: '14'
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MinimumPasswordLength
section: System Access
value: 14
```

Version History

Version ‘r1’: created

WN16-AC-000070

SRG-OS-000069-GPOS-00037

SV-87975

The built-in Windows password complexity policy must be enabled.

The built-in Windows password complexity policy must be enabled.

Description

VulnDiscussion

The use of complex passwords increases their strength against attack. The built-in Windows password complexity policy requires passwords to contain at least three of the four types of characters (numbers, upper- and lower-case letters, and special characters) and prevents the inclusion of user names or parts of user names.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038, SRG-OS-000071-GPOS-00039, SRG-OS-000266-GPOS-00101

Documentable

false

F-79765r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Password must meet complexity requirements” to “Enabled”.

F-79765r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Password Policy\Password must meet complexity requirements
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: PasswordComplexity
section: System Access
value: 1
```

Version History

Version ‘r1’: created

WN16-AC-000080

SRG-OS-000073-GPOS-00041

SV-87977

Reversible password encryption must be disabled.

Reversible password encryption must be disabled.

Description

VulnDiscussion

Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, which are easily compromised. For this reason, this policy must never be enabled.

Documentable

false

F-79767r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> “Store passwords using reversible encryption” to “Disabled”.

F-79767r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: ClearTextPassword
section: System Access
value: 0
```

Version History

Version ‘r1’: created

WN16-AC-000090

SRG-OS-000112-GPOS-00057

SV-88011

Kerberos user logon restrictions must be enforced.

Kerberos user logon restrictions must be enforced.

Description

VulnDiscussion

This policy setting determines whether the Kerberos Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the target computer. The policy is enabled by default, which is the most secure setting for validating that access to target resources is not circumvented.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Documentable

false

F-79801r1 Implementation Example

Configure the policy value in the Default Domain Policy for Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy >> “Enforce user logon restrictions” to “Enabled”.

F-79801r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Kerberos Policy\Enforce user logon restrictions
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: TicketValidateClient
section: Kerberos Policy
value: 1
```

Version History

Version ‘r1’: created

WN16-DC-000020

SRG-OS-000112-GPOS-00057

SV-88013

The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.

The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.

Description

VulnDiscussion

This setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket used to authenticate the connection expires during the connection.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Documentable

false

F-79803r1 Implementation Example

Configure the policy value in the Default Domain Policy for Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy >> “Maximum lifetime for service ticket” to a maximum of “600” minutes, but not “0”, which equates to “Ticket doesn’t expire”.

F-79803r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Kerberos Policy\Maximum lifetime for service ticket
value: 600
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MaxServiceAge
section: Kerberos Policy
value: 600
```

Version History

Version ‘r1’: created

WN16-DC-000030

SRG-OS-000112-GPOS-00057

SV-88015

The Kerberos user ticket lifetime must be limited to 10 hours or less.

The Kerberos user ticket lifetime must be limited to 10 hours or less.

Description

VulnDiscussion

In Kerberos, there are two types of tickets: Ticket Granting Tickets (TGTs) and Service Tickets. Kerberos tickets have a limited lifetime so the time an attacker has to implement an attack is limited. This policy controls how long TGTs can be renewed. With Kerberos, the user's initial authentication to the domain controller results in a TGT, which is then used to request Service Tickets to resources. Upon startup, each computer gets a TGT before requesting a service ticket to the domain controller and any other computers it needs to access. For services that start up under a specified user account, users must always get a TGT first and then get Service Tickets to all computers and services accessed.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Documentable

false

F-79805r1 Implementation Example

Configure the policy value in the Default Domain Policy for Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy >> "Maximum lifetime for user ticket" to a maximum of "10" hours but not "0", which equates to "Ticket doesn't expire".

F-79805r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Kerberos Policy\Maximum lifetime for user ticket
value: 10
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MaxTicketAge
section: Kerberos Policy
value: 10
```

Version History

Version 'r1': created

WN16-DC-000040

SRG-OS-000112-GPOS-00057

SV-88017

The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.

The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.

Description

VulnDiscussion

This setting determines the period of time (in days) during which a user's Ticket Granting Ticket (TGT) may be renewed. This security configuration limits the amount of time an attacker has to crack the TGT and gain access.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Documentable

false

F-79807r1 Implementation Example

Configure the policy value in the Default Domain Policy for Computer Configuration >> Policies >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy >> "Maximum lifetime for user ticket renewal" to a maximum of "7" days or less.

F-79807r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Kerberos Policy\Maximum lifetime for user ticket renewal
value: 7
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MaxRenewAge
section: Kerberos Policy
value: 7
```

Version History

Version 'r1': created

WN16-DC-000050

SRG-OS-000112-GPOS-00057

SV-88019

The computer clock synchronization tolerance must be limited to 5 minutes or less.

The computer clock synchronization tolerance must be limited to 5 minutes or less.

Description

VulnDiscussion

This setting determines the maximum time difference (in minutes) that Kerberos will tolerate between the time on a client's clock and the time on a server's clock while still considering the two clocks synchronous. In order to prevent replay attacks, Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in sync as much as possible.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Documentable

false

F-79809r1 Implementation Example

Configure the policy value in the Default Domain Policy for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Kerberos Policy >> "Maximum tolerance for computer clock synchronization" to a maximum of "5" minutes or less.

F-79809r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Account
  Policies\Kerberos Policy\Maximum tolerance for computer clock synchronization
value: 5
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MaxClockSkew
section: Kerberos Policy
value: 5
```

Version History

Version 'r1': created

WN16-DC-000060

SRG-OS-000324-GPOS-00125

SV-88021

Permissions on the Active Directory data files must only allow System and Administrators access.

Permissions on the Active Directory data files must only allow System and Administrators access.

Description

VulnDiscussion

Improper access permissions for directory data-related files could allow unauthorized users to read, modify, or delete directory data or audit trails.

Documentable

false

F-79811r1 Implementation Example

Maintain the permissions on NTDS database and log files as follows:

NT AUTHORITY:(I)(F) BUILTIN:(I)(F)

I. ◦ permission inherited from parent container

F. ◦ full access

Version History

Version ‘r1’: created

WN16-DC-000070

SRG-OS-000057-GPOS-00027

SV-88057

Permissions for the Application event log must prevent access by non-privileged accounts.

Permissions for the Application event log must prevent access by non-privileged accounts.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The Application event log may be susceptible to tampering if proper permissions are not applied.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Documentable

false

F-79847r1 Implementation Example

Configure the permissions on the Application event log file (Application.evtx) to prevent access by non-privileged accounts. The default permissions listed below satisfy this requirement:

Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control

The default location is the “%SystemRoot% System32” folder.

If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as “NT Service”.

Version History

Version ‘r1’: created

WN16-AU-000030

SRG-OS-000057-GPOS-00027

SV-88059

Permissions for the Security event log must prevent access by non-privileged accounts.

Permissions for the Security event log must prevent access by non-privileged accounts.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The Security event log may disclose sensitive information or be susceptible to tampering if proper permissions are not applied.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Documentable

false

F-79849r1 Implementation Example

Configure the permissions on the Security event log file (Security.evtx) to prevent access by non-privileged accounts. The default permissions listed below satisfy this requirement:

Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control

The default location is the “%SystemRoot% System32” folder.

If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as “NT Service”.

Version History

Version ‘r1’: created

WN16-AU-000040

SRG-OS-000057-GPOS-00027

SV-88061

Permissions for the System event log must prevent access by non-privileged accounts.

Permissions for the System event log must prevent access by non-privileged accounts.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. The System event log may be susceptible to tampering if proper permissions are not applied.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Documentable

false

F-79851r1 Implementation Example

Configure the permissions on the System event log file (System.evtx) to prevent access by non-privileged accounts. The default permissions listed below satisfy this requirement:

Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control

The default location is the “%SystemRoot% System32” folder.

If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as “NT Service”.

Version History

Version ‘r1’: created

WN16-AU-000050

SRG-OS-000257-GPOS-00098

SV-88063

Event Viewer must be protected from unauthorized modification and deletion.

Event Viewer must be protected from unauthorized modification and deletion.

Description

VulnDiscussion

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the modification or deletion of audit tools.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Documentable

false

F-79853r1 Implementation Example

Configure the permissions on the “Eventvwr.exe” file to prevent modification by any groups or accounts other than TrustedInstaller. The default permissions listed below satisfy this requirement:

TrustedInstaller - Full Control Administrators, SYSTEM, Users, ALL APPLICATION PACKAGES, ALL RESTRICTED APPLICATION PACKAGES - Read & Execute

The default location is the “%SystemRoot% System32” folder.

Version History

Version ‘r1’: created

WN16-AU-000060

SRG-OS-000470-GPOS-00214

SV-88065

Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.

Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Credential Validation records events related to validation tests on credentials for a user account logon.

Documentable

false

F-79855r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Logon >> “Audit Credential Validation” with “Success” selected.

F-79855r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE923F-69AE-11D9-BED3-505054503030}'
name: Credential Validation
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000070

SRG-OS-000470-GPOS-00214

SV-88067

Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.

Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Credential Validation records events related to validation tests on credentials for a user account logon.

Documentable

false

F-79857r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Logon >> “Audit Credential Validation” with “Failure” selected.

F-79857r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE923F-69AE-11D9-BED3-505054503030}'
name: Credential Validation
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000080

SRG-OS-000327-GPOS-00127

SV-88071

Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.

Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Other Account Management Events records events such as the access of a password hash or the Password Policy Checking API being called.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Documentable

false

F-79861r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> “Audit Other Account Management Events” with “Success” selected.

F-79861r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE923A-69AE-11D9-BED3-505054503030}'
name: Other Account Management Events
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000100

SRG-OS-000004-GPOS-00004

SV-88075

Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.

Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Security Group Management records events such as creating, deleting, or changing security groups, including changes in group members.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Documentable

false

F-79865r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> “Audit Security Group Management” with “Success” selected.

F-79865r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Account Management\Audit Security
  Group Management
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9237-69AE-11D9-BED3-505054503030}'
name: Security Group Management
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000120

SRG-OS-000004-GPOS-00004

SV-88079

Windows Server 2016 must be configured to audit Account Management - User Account Management successes.

Windows Server 2016 must be configured to audit Account Management - User Account Management successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

User Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling user accounts.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Documentable

false

F-79869r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> “Audit User Account Management” with “Success” selected.

F-79869r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Account Management\Audit User Account
  Management
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9235-69AE-11D9-BED3-505054503030}'
name: User Account Management
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000140

SRG-OS-000004-GPOS-00004

SV-88081

Windows Server 2016 must be configured to audit Account Management - User Account Management failures.

Windows Server 2016 must be configured to audit Account Management - User Account Management failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

User Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling user accounts.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Documentable

false

F-79871r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Account Management >> “Audit User Account Management” with “Failure” selected.

F-79871r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Account Management\Audit User Account
  Management
value: Failure
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9235-69AE-11D9-BED3-505054503030}'
name: User Account Management
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000150

SRG-OS-000327-GPOS-00127

SV-88085

Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.

Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Process Creation records events related to the creation of a process and the source.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215

Documentable

false

F-79875r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> “Audit Process Creation” with “Success” selected.

F-79875r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE922B-69AE-11D9-BED3-505054503030}'
name: Process Creation
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000170

SRG-OS-000327-GPOS-00127

SV-88087

Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.

Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Directory Service Access records events related to users accessing an Active Directory object.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79877r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> DS Access >> “Directory Service Access” with “Success” selected.

F-79877r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE923B-69AE-11D9-BED3-505054503030}'
name: Directory Service Access
value: 1
```

Version History

Version ‘r1’: created

WN16-DC-000240

SRG-OS-000327-GPOS-00127

SV-88089

Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.

Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Directory Service Access records events related to users accessing an Active Directory object.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79879r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> DS Access >> “Directory Service Access” with “Failure” selected.

F-79879r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE923B-69AE-11D9-BED3-505054503030}'
name: Directory Service Access
value: 2
```

Version History

Version ‘r1’: created

WN16-DC-000250

SRG-OS-000327-GPOS-00127

SV-88091

Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.

Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Directory Service Changes records events related to changes made to objects in Active Directory Domain Services.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79881r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> DS Access >> “Directory Service Changes” with “Success” selected.

F-79881r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE923C-69AE-11D9-BED3-505054503030}'
name: Directory Service Changes
value: 1
```

Version History

Version ‘r1’: created

WN16-DC-000260

SRG-OS-000327-GPOS-00127

SV-88093

Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.

Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Directory Service Changes records events related to changes made to objects in Active Directory Domain Services.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79883r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> DS Access >> “Directory Service Changes” with “Failure” selected.

F-79883r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE923C-69AE-11D9-BED3-505054503030}'
name: Directory Service Changes
value: 2
```

Version History

Version ‘r1’: created

WN16-DC-000270

SRG-OS-000240-GPOS-00090

SV-88095

Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.

Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Account Lockout events can be used to identify potentially malicious logon attempts.

Satisfies: SRG-OS-000240-GPOS-00090, SRG-OS-000470-GPOS-00214

Documentable

false

F-79885r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Account Lockout” with “Success” selected.

F-79885r2 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Account Lockout
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9217-69AE-11D9-BED3-505054503030}'
name: Account Lockout
value: 1
```

Version History

Version ‘r3’: created

WN16-AU-000220

SRG-OS-000240-GPOS-00090

SV-88097

Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.

Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Account Lockout events can be used to identify potentially malicious logon attempts.

Satisfies: SRG-OS-000240-GPOS-00090, SRG-OS-000470-GPOS-00214

Documentable

false

F-79887r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Account Lockout” with “Failure” selected.

F-79887r2 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Account Lockout
value: Failure
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9217-69AE-11D9-BED3-505054503030}'
name: Account Lockout
value: 2
```

Version History

Version ‘r3’: created

WN16-AU-000230

SRG-OS-000032-GPOS-00013

SV-88101

Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.

Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Logoff records user logoffs. If this is an interactive logoff, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Documentable

false

F-79891r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Logoff” with “Success” selected.

F-79891r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Logoff
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9216-69AE-11D9-BED3-505054503030}'
name: Logoff
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000250

SRG-OS-000032-GPOS-00013

SV-88103

Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.

Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Logon records user logons. If this is an interactive logon, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Documentable

false

F-79893r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Logon” with “Success” selected.

F-79893r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Logon
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9215-69AE-11D9-BED3-505054503030}'
name: Logon
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000260

SRG-OS-000032-GPOS-00013

SV-88105

Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.

Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Logon records user logons. If this is an interactive logon, it is recorded on the local system. If it is to a network share, it is recorded on the system accessed.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Documentable

false

F-79895r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Logon” with “Failure” selected.

F-79895r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Logon
value: Failure
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9215-69AE-11D9-BED3-505054503030}'
name: Logon
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000270

SRG-OS-000470-GPOS-00214

SV-88107

Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.

Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Special Logon records special logons that have administrative privileges and can be used to elevate processes.

Satisfies: SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Documentable

false

F-79897r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> “Audit Special Logon” with “Success” selected.

F-79897r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Logon/Logoff\Audit Special Logon
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE921B-69AE-11D9-BED3-505054503030}'
name: Special Logon
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000280

SRG-OS-000327-GPOS-00127

SV-88113

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Policy Change records events related to changes in audit policy.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79903r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> “Audit Audit Policy Change” with “Success” selected.

F-79903r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Policy Change\Audit Audit Policy
  Change
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE922F-69AE-11D9-BED3-505054503030}'
name: Audit Policy Change
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000310

SRG-OS-000327-GPOS-00127

SV-88115

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.

Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Policy Change records events related to changes in audit policy.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79905r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> “Audit Audit Policy Change” with “Failure” selected.

F-79905r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Policy Change\Audit Audit Policy
  Change
value: Failure
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE922F-69AE-11D9-BED3-505054503030}'
name: Audit Policy Change
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000320

SRG-OS-000327-GPOS-00127

SV-88117

Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.

Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Authentication Policy Change records events related to changes in authentication policy, including Kerberos policy and Trust changes.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Documentable

false

F-79907r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> “Audit Authentication Policy Change” with “Success” selected.

F-79907r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Policy Change\Audit Authentication
  Policy Change
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9230-69AE-11D9-BED3-505054503030}'
name: Authentication Policy Change
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000330

SRG-OS-000327-GPOS-00127

SV-88119

Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.

Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Authorization Policy Change records events related to changes in user rights, such as “Create a token object”.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Documentable

false

F-79909r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> “Audit Authorization Policy Change” with “Success” selected.

F-79909r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Policy Change\Audit Authorization
  Policy Change
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9231-69AE-11D9-BED3-505054503030}'
name: Authorization Policy Change
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000340

SRG-OS-000327-GPOS-00127

SV-88121

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Sensitive Privilege Use records events related to use of sensitive privileges, such as “Act as part of the operating system” or “Debug programs”.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Documentable

false

F-79911r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> “Audit Sensitive Privilege Use” with “Success” selected.

F-79911r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Privilege Use\Audit Sensitive Privilege
  Use
value: Success
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9228-69AE-11D9-BED3-505054503030}'
name: Sensitive Privilege Use
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000350

SRG-OS-000327-GPOS-00127

SV-88123

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.

Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Sensitive Privilege Use records events related to use of sensitive privileges, such as “Act as part of the operating system” or “Debug programs”.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210

Documentable

false

F-79913r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Privilege Use >> “Audit Sensitive Privilege Use” with “Failure” selected.

F-79913r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
  Audit Policy Configuration\System Audit Policies\Privilege Use\Audit Sensitive Privilege
  Use
value: Failure
```

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9228-69AE-11D9-BED3-505054503030}'
name: Sensitive Privilege Use
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000360

SRG-OS-000327-GPOS-00127

SV-88125

Windows Server 2016 must be configured to audit System - IPsec Driver successes.

Windows Server 2016 must be configured to audit System - IPsec Driver successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

IPsec Driver records events related to the IPsec Driver, such as dropped packets.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79915r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit IPsec Driver” with “Success” selected.

F-79915r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9213-69AE-11D9-BED3-505054503030}'
name: IPsec Driver
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000370

SRG-OS-000327-GPOS-00127

SV-88127

Windows Server 2016 must be configured to audit System - IPsec Driver failures.

Windows Server 2016 must be configured to audit System - IPsec Driver failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

IPsec Driver records events related to the IPsec Driver, such as dropped packets.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79917r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit IPsec Driver” with “Failure” selected.

F-79917r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9213-69AE-11D9-BED3-505054503030}'
name: IPsec Driver
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000380

SRG-OS-000327-GPOS-00127

SV-88129

Windows Server 2016 must be configured to audit System - Other System Events successes.

Windows Server 2016 must be configured to audit System - Other System Events successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Other System Events records information related to cryptographic key operations and the Windows Firewall service.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79919r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit Other System Events” with “Success” selected.

F-79919r2 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9214-69AE-11D9-BED3-505054503030}'
name: Other System Events
value: 1
```

Version History

Version ‘r3’: created

WN16-AU-000390

SRG-OS-000327-GPOS-00127

SV-88131

Windows Server 2016 must be configured to audit System - Other System Events failures.

Windows Server 2016 must be configured to audit System - Other System Events failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Audit Other System Events records information related to cryptographic key operations and the Windows Firewall service.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79921r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit Other System Events” with “Failure” selected.

F-79921r2 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9214-69AE-11D9-BED3-505054503030}'
name: Other System Events
value: 2
```

Version History

Version ‘r3’: created

WN16-AU-000400

SRG-OS-000327-GPOS-00127

SV-88133

Windows Server 2016 must be configured to audit System - Security State Change successes.

Windows Server 2016 must be configured to audit System - Security State Change successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Security State Change records events related to changes in the security state, such as startup and shutdown of the system.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79923r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit Security State Change” with “Success” selected.

F-79923r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9210-69AE-11D9-BED3-505054503030}'
name: Security State Change
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000410

SRG-OS-000327-GPOS-00127

SV-88135

Windows Server 2016 must be configured to audit System - Security System Extension successes.

Windows Server 2016 must be configured to audit System - Security System Extension successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Security System Extension records events related to extension code being loaded by the security subsystem.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212

Documentable

false

F-79925r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit Security System Extension” with “Success” selected.

F-79925r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9211-69AE-11D9-BED3-505054503030}'
name: Security System Extension
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000420

SRG-OS-000134-GPOS-00068

SV-88139

Administrator accounts must not be enumerated during elevation.

Administrator accounts must not be enumerated during elevation.

Description

VulnDiscussion

Enumeration of administrator accounts when elevating can provide part of the logon information to an unauthorized user. This setting configures the system to always require users to type in a username and password to elevate a running application.

Documentable

false

F-79929r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Credential User Interface >> “Enumerate administrator accounts on elevation” to “Disabled”.

F-79929r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Credential
  User Interface\Enumerate administrator accounts on elevation
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\CredUI
value_name: EnumerateAdministrators
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000280

SRG-OS-000327-GPOS-00127

SV-88141

Windows Server 2016 must be configured to audit System - System Integrity successes.

Windows Server 2016 must be configured to audit System - System Integrity successes.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

System Integrity records events related to violations of integrity to the security subsystem.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Documentable

false

F-79931r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit System Integrity” with “Success” selected.

F-79931r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Success
guid: '{0CCE9212-69AE-11D9-BED3-505054503030}'
name: System Integrity
value: 1
```

Version History

Version ‘r1’: created

WN16-AU-000440

SRG-OS-000327-GPOS-00127

SV-88143

Windows Server 2016 must be configured to audit System - System Integrity failures.

Windows Server 2016 must be configured to audit System - System Integrity failures.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

System Integrity records events related to violations of integrity to the security subsystem.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Documentable

false

F-79933r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> System >> “Audit System Integrity” with “Failure” selected.

F-79933r1 Machine readable information

Windows GPO Setting

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

Windows Audit Configuration

```
system: org.scapolite.implementation.win_audit
string_value: Failure
guid: '{0CCE9212-69AE-11D9-BED3-505054503030}'
name: System Integrity
value: 2
```

Version History

Version ‘r1’: created

WN16-AU-000450

SRG-OS-000095-GPOS-00049

SV-88145

The display of slide shows on the lock screen must be disabled.

The display of slide shows on the lock screen must be disabled.

Description

VulnDiscussion

Slide shows that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged-on user.

Documentable

false

F-79935r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> “Prevent enabling lock screen slide show” to “Enabled”.

F-79935r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Control Panel\Personalization\Prevent
  enabling lock screen slide show
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Personalization
value_name: NoLockScreenSlideshow
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000010

SRG-OS-000134-GPOS-00068

SV-88147

Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.

Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.

Description

VulnDiscussion

A compromised local administrator account can provide means for an attacker to move laterally between domain systems.

With User Account Control enabled, filtering the privileged token for local administrator accounts will prevent the elevated privileges of these accounts from being used over the network.

Documentable

false

F-79937r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> “Apply UAC restrictions to local accounts on network logons” to “Enabled”.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package. “SecGuide.admx” and " SecGuide.adml" must be copied to the and -US directories respectively.

F-79937r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\MS Security Guide\Apply UAC
  restrictions to local accounts on network logons
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
value_name: LocalAccountTokenFilterPolicy
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-MS-000020

SRG-OS-000095-GPOS-00049

SV-88149

WDigest Authentication must be disabled.

WDigest Authentication must be disabled.

Description

VulnDiscussion

When the WDigest Authentication protocol is enabled, plain-text passwords are stored in the Local Security Authority Subsystem Service (LSASS), exposing them to theft. WDigest is disabled by default in Windows 10. This setting ensures this is enforced.

Documentable

false

F-79939r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> “WDigest Authentication (disabling may require KB2871997)” to “Disabled”.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package. “SecGuide.admx” and " SecGuide.adml" must be copied to the and -US directories respectively.

F-79939r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\MS Security Guide\WDigest
  Authentication (disabling may require KB2871997)
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
value_name: UseLogonCredential
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000030

SRG-OS-000480-GPOS-00227

SV-88151

Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.

Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.

Description

VulnDiscussion

Configuring the system to disable IPv6 source routing protects against spoofing.

Documentable

false

F-79941r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> “MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)” to “Enabled” with “Highest protection, source routing is completely disabled” selected.

This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. “MSS-Legacy.admx” and “MSS-Legacy.adml” must be copied to the and -US directories respectively.

F-79941r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting
  IPv6) IP source routing protection level (protects against packet spoofing)'
value: Highest protection, source routing is completely disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: System\CurrentControlSet\Services\Tcpip6\Parameters
value_name: DisableIPSourceRouting
action: DWORD:2
```

Version History

Version ‘r1’: created

WN16-CC-000040

SRG-OS-000480-GPOS-00227

SV-88153

Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.

Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.

Description

VulnDiscussion

Configuring the system to disable IP source routing protects against spoofing.

Documentable

false

F-79943r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> “MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)” to “Enabled” with “Highest protection, source routing is completely disabled” selected.

This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. “MSS-Legacy.admx” and “MSS-Legacy.adml” must be copied to the and -US directories respectively.

F-79943r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting)
  IP source routing protection level (protects against packet spoofing)'
value: Highest protection, source routing is completely disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: System\CurrentControlSet\Services\Tcpip\Parameters
value_name: DisableIPSourceRouting
action: DWORD:2
```

Version History

Version ‘r1’: created

WN16-CC-000050

SRG-OS-000480-GPOS-00227

SV-88155

Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.

Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.

Description

VulnDiscussion

Allowing ICMP redirect of routes can lead to traffic not being routed properly. When disabled, this forces ICMP to be routed via the shortest path first.

Documentable

false

F-79945r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> “MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes” to “Disabled”.

This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. “MSS-Legacy.admx” and “MSS-Legacy.adml” must be copied to the and -US directories respectively.

F-79945r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect)
  Allow ICMP redirects to override OSPF generated routes'
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: System\CurrentControlSet\Services\Tcpip\Parameters
value_name: EnableICMPRedirect
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000060

SRG-OS-000420-GPOS-00186

SV-88157

Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.

Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.

Description

VulnDiscussion

Configuring the system to ignore name release requests, except from WINS servers, prevents a denial of service (DoS) attack. The DoS consists of sending a NetBIOS name release request to the server for each entry in the server's cache, causing a response delay in the normal operation of the server's WINS resolution capability.

Documentable

false

F-79947r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" to "Enabled".

This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. "MSS-Legacy.admx" and "MSS-Legacy.adml" must be copied to the and -US directories respectively.

F-79947r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand)
  Allow the computer to ignore NetBIOS name release requests except from WINS servers'
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: System\CurrentControlSet\Services\Netbt\Parameters
value_name: NoNameReleaseOnDemand
action: DWORD:1
```

Version History

Version 'r1': created

WN16-CC-000070

SRG-OS-000480-GPOS-00227

SV-88159

Insecure logons to an SMB server must be disabled.

Insecure logons to an SMB server must be disabled.

Description

VulnDiscussion

Insecure guest logons allow unauthenticated access to shared folders. Shared resources on a system must require authentication to establish proper access.

Documentable

false

F-79949r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Lanman Workstation >> “Enable insecure guest logons” to “Disabled”.

F-79949r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Network\Lanman Workstation\Enable
  insecure guest logons
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\LanmanWorkstation
value_name: AllowInsecureGuestAuth
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000080

SRG-OS-000480-GPOS-00227

SV-88161

Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *and* \shares.

Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *and* \shares.

Description

VulnDiscussion

Additional security requirements are applied to Universal Naming Convention (UNC) paths specified in hardened UNC paths before allowing access to them. This aids in preventing tampering with or spoofing of connections to these paths.

Documentable

false

F-79951r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Provider >> “Hardened UNC Paths” to “Enabled” with at least the following configured in “Hardened UNC Paths”: (click the “Show” button to display)

Value Name: * Value: RequireMutualAuthentication=1, RequireIntegrity=1

Value Name: * Value: RequireMutualAuthentication=1, RequireIntegrity=1

F-79951r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Network\Network Provider\Hardened
  UNC Paths
value:
  \\*\SYSVOL: RequireMutualAuthentication=1, RequireIntegrity=1
  \\*\NETLOGON: RequireMutualAuthentication=1, RequireIntegrity=1
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
value_name: \\*\SYSVOL
action: SZ:RequireMutualAuthentication=1, RequireIntegrity=1
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
value_name: \\*\NETLOGON
action: SZ:RequireMutualAuthentication=1, RequireIntegrity=1
```

Version History

Version ‘r1’: created

WN16-CC-000090

SRG-OS-000042-GPOS-00020

SV-88163

Command line data must be included in process creation events.

Command line data must be included in process creation events.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Enabling “Include command line data for process creation events” will record the command line information with the process creation events in the log. This can provide additional detail when malware has run on a system.

Documentable

false

F-79953r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Audit Process Creation >> “Include command line in process creation events” to “Enabled”.

F-79953r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Audit Process Creation\Include
  command line in process creation events
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit
value_name: ProcessCreationIncludeCmdLine_Enabled
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000100

SRG-OS-000480-GPOS-00227

SV-88173

Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.

Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.

Description

VulnDiscussion

Compromised boot drivers can introduce malware prior to protection mechanisms that load after initialization. The Early Launch Antimalware driver can limit allowed drivers based on classifications determined by the malware protection application. At a minimum, drivers determined to be bad must not be allowed.

Documentable

false

F-79961r1 Implementation Example

The default behavior is for Early Launch Antimalware - Boot-Start Driver Initialization policy to enforce “Good, unknown and bad but critical” (preventing “bad”).

If this needs to be corrected or a more secure setting is desired, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Early Launch Antimalware >> “Boot-Start Driver Initialization Policy” to “Not Configured” or “Enabled” with any option other than “All” selected.

F-79961r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration \ Administrative Templates\System\Early Launch Antimalware\Boot-Start
  Driver Initialization Policy
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: System\CurrentControlSet\Policies\EarlyLaunch
value_name: DriverLoadPolicy
action: DWORD:NOT_SET
```

Version History

Version ‘r1’: created

WN16-CC-000140

SRG-OS-000480-GPOS-00227

SV-88177

Group Policy objects must be reprocessed even if they have not changed.

Group Policy objects must be reprocessed even if they have not changed.

Description

VulnDiscussion

Registry entries for group policy settings can potentially be changed from the required configuration. This could occur as part of troubleshooting or by a malicious process on a compromised system. Enabling this setting and then selecting the “Process even if the Group Policy objects have not changed” option ensures the policies will be reprocessed even if none have been changed. This way, any unauthorized changes are forced to match the domain-based group policy settings again.

Documentable

false

F-79965r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Group Policy >> “Configure registry policy processing” to “Enabled” with the option “Process even if the Group Policy objects have not changed” selected.

F-79965r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Group Policy\Configure
  registry policy processing
value:
  Process even if the Group Policy objects have not changed: Enabled
  Do not apply during periodic background processing: Disabled
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
value_name: NoBackgroundPolicy
action: DWORD:0
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
value_name: NoGPOListChanges
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000150

SRG-OS-000095-GPOS-00049

SV-88179

Downloading print driver packages over HTTP must be prevented.

Downloading print driver packages over HTTP must be prevented.

Description

VulnDiscussion

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and will prevent uncontrolled updates to the system.

This setting prevents the computer from downloading print driver packages over HTTP.

Documentable

false

F-79969r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> “Turn off downloading of print drivers over HTTP” to “Enabled”.

F-79969r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Internet Communication
  Management\Internet Communication settings\Turn off downloading of print drivers
  over HTTP
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows NT\Printers
value_name: DisableWebPnPDownload
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000160

SRG-OS-000095-GPOS-00049

SV-88181

Printing over HTTP must be prevented.

Printing over HTTP must be prevented.

Description

VulnDiscussion

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and will prevent uncontrolled updates to the system.

This setting prevents the client computer from printing over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.

Documentable

false

F-79971r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> “Turn off printing over HTTP” to “Enabled”.

F-79971r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Internet Communication
  Management\Internet Communication settings\Turn off printing over HTTP
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows NT\Printers
value_name: DisableHTTPPrinting
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000170

SRG-OS-000095-GPOS-00049

SV-88185

The network selection user interface (UI) must not be displayed on the logon screen.

The network selection user interface (UI) must not be displayed on the logon screen.

Description

VulnDiscussion

Enabling interaction with the network selection UI allows users to change connections to available networks without signing in to Windows.

Documentable

false

F-79973r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> “Do not display network selection UI” to “Enabled”.

F-79973r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Logon\Do not display
  network selection UI
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\System
value_name: DontDisplayNetworkSelectionUI
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000180

SRG-OS-000095-GPOS-00049

SV-88187

Local users on domain-joined computers must not be enumerated.

Local users on domain-joined computers must not be enumerated.

Description

VulnDiscussion

The username is one part of logon credentials that could be used to gain access to a system. Preventing the enumeration of users limits this information to authorized personnel.

Documentable

false

F-79975r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> “Enumerate local users on domain-joined computers” to “Disabled”.

F-79975r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Logon\Enumerate local
  users on domain-joined computers
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\System
value_name: EnumerateLocalUsers
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-MS-000030

SRG-OS-000480-GPOS-00227

SV-88197

Users must be prompted to authenticate when the system wakes from sleep (on battery).

Users must be prompted to authenticate when the system wakes from sleep (on battery).

Description

VulnDiscussion

A system that does not require authentication when resuming from sleep may provide access to unauthorized users. Authentication must always be required when accessing a system. This setting ensures users are prompted for a password when the system wakes from sleep (on battery).

Documentable

false

F-79979r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Power Management >> Sleep Settings >> “Require a password when a computer wakes (on battery)” to “Enabled”.

F-79979r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Power Management\Sleep
  Settings\Require a password when a computer wakes (on battery)
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51
value_name: DCSettingIndex
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000210

SRG-OS-000480-GPOS-00227

SV-88201

Users must be prompted to authenticate when the system wakes from sleep (plugged in).

Users must be prompted to authenticate when the system wakes from sleep (plugged in).

Description

VulnDiscussion

A system that does not require authentication when resuming from sleep may provide access to unauthorized users. Authentication must always be required when accessing a system. This setting ensures users are prompted for a password when the system wakes from sleep (plugged in).

Documentable

false

F-79981r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Power Management >> Sleep Settings >> “Require a password when a computer wakes (plugged in)” to “Enabled”.

F-79981r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Power Management\Sleep
  Settings\Require a password when a computer wakes (plugged in)
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51
value_name: ACSettingIndex
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000220

SRG-OS-000379-GPOS-00164

SV-88203

Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.

Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.

Description

VulnDiscussion

Unauthenticated RPC clients may allow anonymous access to sensitive information. Configuring RPC to restrict unauthenticated RPC clients from connecting to the RPC server will prevent anonymous connections.

Documentable

false

F-79983r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Procedure Call >> “Restrict Unauthenticated RPC clients” to “Enabled” with “Authenticated” selected.

F-79983r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\System\Remote Procedure Call\Restrict
  Unauthenticated RPC clients
value: Authenticated
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows NT\Rpc
value_name: RestrictRemoteClients
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-MS-000040

SRG-OS-000095-GPOS-00049

SV-88207

The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

Description

VulnDiscussion

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise and will prevent uncontrolled updates to the system.

This setting will prevent the Program Inventory from collecting data about a system and sending the information to Microsoft.

Documentable

false

F-79985r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Application Compatibility >> “Turn off Inventory Collector” to “Enabled”.

F-79985r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Application
  Compatibility\Turn off Inventory Collector
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\AppCompat
value_name: DisableInventory
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000240

SRG-OS-000368-GPOS-00154

SV-88209

AutoPlay must be turned off for non-volume devices.

AutoPlay must be turned off for non-volume devices.

Description

VulnDiscussion

Allowing AutoPlay to execute may introduce malicious code to a system. AutoPlay begins reading from a drive as soon as media is inserted into the drive. As a result, the setup file of programs or music on audio media may start. This setting will disable AutoPlay for non-volume devices, such as Media Transfer Protocol (MTP) devices.

Documentable

false

F-79991r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> “Disallow Autoplay for non-volume devices” to “Enabled”.

F-79991r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\AutoPlay
  Policies\Disallow Autoplay for non-volume devices
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows\Explorer
value_name: NoAutoplayfornonVolume
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000250

SRG-OS-000368-GPOS-00154

SV-88211

The default AutoRun behavior must be configured to prevent AutoRun commands.

The default AutoRun behavior must be configured to prevent AutoRun commands.

Description

VulnDiscussion

Allowing AutoRun commands to execute may introduce malicious code to a system. Configuring this setting prevents AutoRun commands from executing.

Documentable

false

F-79997r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> “Set the default behavior for AutoRun” to “Enabled” with “Do not execute any autorun commands” selected.

F-79997r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\AutoPlay
  Policies\Set the default behavior for AutoRun
value: Do not execute any autorun commands
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
value_name: NoAutorun
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000260

SRG-OS-000368-GPOS-00154

SV-88213

AutoPlay must be disabled for all drives.

AutoPlay must be disabled for all drives.

Description

VulnDiscussion

Allowing AutoPlay to execute may introduce malicious code to a system. AutoPlay begins reading from a drive as soon media is inserted into the drive. As a result, the setup file of programs or music on audio media may start. By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives. Enabling this policy disables AutoPlay on all drives.

Documentable

false

F-79999r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> “Turn off AutoPlay” to “Enabled” with “All Drives” selected.

F-79999r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\AutoPlay
  Policies\Turn off Autoplay
value: All Drives
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
value_name: NoDriveTypeAutoRun
action: DWORD:255
```

Version History

Version ‘r1’: created

WN16-CC-000270

SRG-OS-000480-GPOS-00227

SV-88215

Windows Telemetry must be configured to Security or Basic.

Windows Telemetry must be configured to Security or Basic.

Description

VulnDiscussion

Some features may communicate with the vendor, sending system information or downloading data or components for the feature. Limiting this capability will prevent potentially sensitive information from being sent outside the enterprise. The “Security” option for Telemetry configures the lowest amount of data, effectively none outside of the Malicious Software Removal Tool (MSRT), Defender, and telemetry client settings. “Basic” sends basic diagnostic and usage data and may be required to support some Microsoft services.

Documentable

false

F-80001r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds>> “Allow Telemetry” to “Enabled” with “0 - Security [Enterprise Only]” or “1 - Basic” selected in “Options”.

F-80001r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Data Collection
  and Preview Builds\Allow Telemetry
value: 0 - Security [Enterprise Only]
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows\DataCollection
value_name: AllowTelemetry
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000290

SRG-OS-000341-GPOS-00132

SV-88217

The Application event log size must be configured to 32768 KB or greater.

The Application event log size must be configured to 32768 KB or greater.

Description

VulnDiscussion

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Documentable

false

F-80003r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> Application >> “Specify the maximum log file size (KB)” to “Enabled” with a “Maximum Log Size (KB)” of “32768” or greater.

F-80003r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Event
  Log Service\Application\Specify the maximum log file size (KB)
value: '32768'
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\EventLog\Application
value_name: MaxSize
action: DWORD:32768
```

Version History

Version ‘r1’: created

WN16-CC-000300

SRG-OS-000341-GPOS-00132

SV-88219

The Security event log size must be configured to 196608 KB or greater.

The Security event log size must be configured to 196608 KB or greater.

Description

VulnDiscussion

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Documentable

false

F-80005r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> Security >> “Specify the maximum log file size (KB)” to “Enabled” with a “Maximum Log Size (KB)” of “196608” or greater.

F-80005r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Event
  Log Service\Security\Specify the maximum log file size (KB)
value: '196608'
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\EventLog\Security
value_name: MaxSize
action: DWORD:196608
```

Version History

Version ‘r1’: created

WN16-CC-000310

SRG-OS-000341-GPOS-00132

SV-88221

The System event log size must be configured to 32768 KB or greater.

The System event log size must be configured to 32768 KB or greater.

Description

VulnDiscussion

Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel.

Documentable

false

F-80007r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Event Log Service >> System >> “Specify the maximum log file size (KB)” to “Enabled” with a “Maximum Log Size (KB)” of “32768” or greater.

F-80007r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Event
  Log Service\System\Specify the maximum log file size (KB)
value: '32768'
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\EventLog\System
value_name: MaxSize
action: DWORD:32768
```

Version History

Version ‘r1’: created

WN16-CC-000320

SRG-OS-000095-GPOS-00049

SV-88223

Windows SmartScreen must be enabled.

Windows SmartScreen must be enabled.

Description

VulnDiscussion

Windows SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling SmartScreen will warn users of potentially malicious programs.

Documentable

false

F-80009r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> “Configure Windows SmartScreen” to “Enabled”.

F-80009r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\File Explorer\Configure
  Windows SmartScreen
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\System
value_name: EnableSmartScreen
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000330

SRG-OS-000433-GPOS-00192

SV-88225

Explorer Data Execution Prevention must be enabled.

Explorer Data Execution Prevention must be enabled.

Description

VulnDiscussion

Data Execution Prevention provides additional protection by performing checks on memory to help prevent malicious code from running. This setting will prevent Data Execution Prevention from being turned off for File Explorer.

Documentable

false

F-80011r1 Implementation Example

The default behavior is for data execution prevention to be turned on for File Explorer.

If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> “Turn off Data Execution Prevention for Explorer” to “Not Configured” or “Disabled”.

F-80011r1 Machine readable information

Windows GPO Setting

```
ui_path: this needs to be corrected , configure the policy value for Computer Configuration\Administrative
  Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for
  Explorer
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Explorer
value_name: NoDataExecutionPrevention
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000340

SRG-OS-000480-GPOS-00227

SV-88227

Turning off File Explorer heap termination on corruption must be disabled.

Turning off File Explorer heap termination on corruption must be disabled.

Description

VulnDiscussion

Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this.

Documentable

false

F-80013r1 Implementation Example

The default behavior is for File Explorer heap termination on corruption to be disabled.

If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> “Turn off heap termination on corruption” to “Not Configured” or “Disabled”.

F-80013r1 Machine readable information

Windows GPO Setting

```
ui_path: this needs to be corrected , configure the policy value for Computer Configuration\Administrative
  Templates\Windows Components\File Explorer\Turn off heap termination on corruption
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Explorer
value_name: NoHeapTerminationOnCorruption
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000350

SRG-OS-000480-GPOS-00227

SV-88229

File Explorer shell protocol must run in protected mode.

File Explorer shell protocol must run in protected mode.

Description

VulnDiscussion

The shell protocol will limit the set of folders that applications can open when run in protected mode. Restricting files an application can open to a limited set of folders increases the security of Windows.

Documentable

false

F-80015r1 Implementation Example

The default behavior is for shell protected mode to be turned on for File Explorer.

If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> “Turn off shell protocol protected mode” to “Not Configured” or “Disabled”.

F-80015r1 Machine readable information

Windows GPO Setting

```
ui_path: this needs to be corrected , configure the policy value for Computer Configuration\Administrative
  Templates\Windows Components\File Explorer\Turn off shell protocol protected mode
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
value_name: PreXPSP2ShellProtocolBehavior
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000360

SRG-OS-000373-GPOS-00157

SV-88231

Passwords must not be saved in the Remote Desktop Client.

Passwords must not be saved in the Remote Desktop Client.

Description

VulnDiscussion

Saving passwords in the Remote Desktop Client could allow an unauthorized user to establish a remote desktop session to another system. The system must be configured to prevent users from saving passwords in the Remote Desktop Client.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80017r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Connection Client >> “Do not allow passwords to be saved” to “Enabled”.

F-80017r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Remote
  Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: DisablePasswordSaving
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000370

SRG-OS-000138-GPOS-00069

SV-88233

Local drives must be prevented from sharing with Remote Desktop Session Hosts.

Local drives must be prevented from sharing with Remote Desktop Session Hosts.

Description

VulnDiscussion

Preventing users from sharing the local drives on their client computers with Remote Session Hosts that they access helps reduce possible exposure of sensitive data.

Documentable

false

F-80019r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Device and Resource Redirection >> “Do not allow drive redirection” to “Enabled”.

F-80019r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Remote
  Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do
  not allow drive redirection
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: fDisableCdm
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000380

SRG-OS-000373-GPOS-00157

SV-88235

Remote Desktop Services must always prompt a client for passwords upon connection.

Remote Desktop Services must always prompt a client for passwords upon connection.

Description

VulnDiscussion

This setting controls the ability of users to supply passwords automatically as part of their remote desktop connection. Disabling this setting would allow anyone to use the stored credentials in a connection item to connect to the terminal server.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80021r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> “Always prompt for password upon connection” to “Enabled”.

F-80021r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Remote
  Desktop Services\Remote Desktop Session Host\Security\Always prompt for password
  upon connection
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: fPromptForPassword
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000390

SRG-OS-000250-GPOS-00093

SV-88237

The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.

The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.

Description

VulnDiscussion

Allowing unsecure RPC communication exposes the system to man-in-the-middle attacks and data disclosure attacks. A man-in-the-middle attack occurs when an intruder captures packets between a client and server and modifies them before allowing the packets to be exchanged. Usually the attacker will modify the information in the packets in an attempt to cause either the client or server to reveal sensitive information.

Documentable

false

F-80023r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> “Require secure RPC communication” to “Enabled”.

F-80023r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Remote
  Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: fEncryptRPCTraffic
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000400

SRG-OS-000250-GPOS-00093

SV-88239

Remote Desktop Services must be configured with the client connection encryption set to High Level.

Remote Desktop Services must be configured with the client connection encryption set to High Level.

Description

VulnDiscussion

Remote connections must be encrypted to prevent interception of data or sensitive information. Selecting “High Level” will ensure encryption of Remote Desktop Services sessions in both directions.

Documentable

false

F-80025r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> “Set client connection encryption level” to “Enabled” with “High Level” selected.

F-80025r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Remote
  Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption
  level
value: High Level
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
value_name: MinEncryptionLevel
action: DWORD:3
```

Version History

Version ‘r1’: created

WN16-CC-000410

SRG-OS-000480-GPOS-00227

SV-88241

Attachments must be prevented from being downloaded from RSS feeds.

Attachments must be prevented from being downloaded from RSS feeds.

Description

VulnDiscussion

Attachments from RSS feeds may not be secure. This setting will prevent attachments from being downloaded from RSS feeds.

Documentable

false

F-80027r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> “Prevent downloading of enclosures” to “Enabled”.

F-80027r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\RSS Feeds\Prevent
  downloading of enclosures
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Internet Explorer\Feeds
value_name: DisableEnclosureDownload
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000420

SRG-OS-000095-GPOS-00049

SV-88243

Basic authentication for RSS feeds over HTTP must not be used.

Basic authentication for RSS feeds over HTTP must not be used.

Description

VulnDiscussion

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Documentable

false

F-80029r1 Implementation Example

The default behavior is for the Windows RSS platform to not use Basic authentication over HTTP connections.

If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> “Turn on Basic feed authentication over HTTP” to “Not Configured” or “Disabled”.

F-80029r1 Machine readable information

Windows GPO Setting

```
ui_path: this needs to be corrected , configure the policy value for Computer Configuration\Administrative
  Templates\Windows Components\RSS Feeds\Turn on Basic feed authentication over HTTP
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Internet Explorer\Feeds
value_name: AllowBasicAuthInClear
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000430

SRG-OS-000095-GPOS-00049

SV-88245

Indexing of encrypted files must be turned off.

Indexing of encrypted files must be turned off.

Description

VulnDiscussion

Indexing of encrypted files may expose sensitive data. This setting prevents encrypted files from being indexed.

Documentable

false

F-80031r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Search >> “Allow indexing of encrypted files” to “Disabled”.

F-80031r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Search\Allow
  indexing of encrypted files
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SOFTWARE\Policies\Microsoft\Windows\Windows Search
value_name: AllowIndexingEncryptedStoresOrItems
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000440

SRG-OS-000362-GPOS-00149

SV-88247

Users must be prevented from changing installation options.

Users must be prevented from changing installation options.

Description

VulnDiscussion

Installation options for applications are typically controlled by administrators. This setting prevents users from changing installation options that may bypass security features.

Documentable

false

F-80033r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> “Allow user control over installs” to “Disabled”.

F-80033r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Installer\Allow user control over installs
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Installer
value_name: EnableUserControl
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000450

SRG-OS-000362-GPOS-00149

SV-88249

The Windows Installer Always install with elevated privileges option must be disabled.

The Windows Installer Always install with elevated privileges option must be disabled.

Description

VulnDiscussion

Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

Documentable

false

F-80035r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> “Always install with elevated privileges” to “Disabled”.

F-80035r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Installer\Always install with elevated privileges
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows\Installer
value_name: AlwaysInstallElevated
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000460

SRG-OS-000480-GPOS-00227

SV-88251

Users must be notified if a web-based program attempts to install software.

Users must be notified if a web-based program attempts to install software.

Description

VulnDiscussion

Web-based programs may attempt to install malicious software on a system. Ensuring users are notified if a web-based program attempts to install software allows them to refuse the installation.

Documentable

false

F-80037r1 Implementation Example

The default behavior is for Internet Explorer to warn users and select whether to allow or refuse installation when a web-based program attempts to install software on the system.

If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> “Prevent Internet Explorer security prompt for Windows Installer scripts” to “Not Configured” or “Disabled”.

F-80037r1 Machine readable information

Windows GPO Setting

```
ui_path: this needs to be corrected , configure the policy value for Computer Configuration\Administrative
  Templates\Windows Components\Windows Installer\Prevent Internet Explorer security
  prompt for Windows Installer scripts
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\Installer
value_name: SafeForScripting
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000470

SRG-OS-000480-GPOS-00229

SV-88253

Automatically signing in the last interactive user after a system-initiated restart must be disabled.

Automatically signing in the last interactive user after a system-initiated restart must be disabled.

Description

VulnDiscussion

Windows can be configured to automatically sign the user back in after a Windows Update restart. Some protections are in place to help ensure this is done in a secure fashion; however, disabling this will prevent the caching of credentials for this purpose and also ensure the user is aware of the restart.

Documentable

false

F-80039r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Logon Options >> “Sign-in last interactive user automatically after a system-initiated restart” to “Disabled”.

F-80039r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Logon Options\Sign-in last interactive user automatically after a system-initiated
  restart
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Microsoft\Windows\CurrentVersion\Policies\System
value_name: DisableAutomaticRestartSignOn
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000480

SRG-OS-000042-GPOS-00020

SV-88255

PowerShell script block logging must be enabled.

PowerShell script block logging must be enabled.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Enabling PowerShell script block logging will record detailed information from the processing of PowerShell commands and scripts. This can provide additional detail when malware has run on a system.

Documentable

false

F-80041r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> “Turn on PowerShell Script Block Logging” to “Enabled”.

F-80041r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  PowerShell\Turn on PowerShell Script Block Logging
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
value_name: EnableScriptBlockLogging
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000490

SRG-OS-000125-GPOS-00065

SV-88257

The Windows Remote Management (WinRM) client must not use Basic authentication.

The Windows Remote Management (WinRM) client must not use Basic authentication.

Description

VulnDiscussion

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Documentable

false

F-80043r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> “Allow Basic authentication” to “Disabled”.

F-80043r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Client\Allow Basic authentication
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Client
value_name: AllowBasic
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000500

SRG-OS-000393-GPOS-00173

SV-88259

The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

Description

VulnDiscussion

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Documentable

false

F-80045r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> “Allow unencrypted traffic” to “Disabled”.

F-80045r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Client
value_name: AllowUnencryptedTraffic
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000510

SRG-OS-000125-GPOS-00065

SV-88261

The Windows Remote Management (WinRM) client must not use Digest authentication.

The Windows Remote Management (WinRM) client must not use Digest authentication.

Description

VulnDiscussion

Digest authentication is not as strong as other options and may be subject to man-in-the-middle attacks. Disallowing Digest authentication will reduce this potential.

Documentable

false

F-80047r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> “Disallow Digest authentication” to “Enabled”.

F-80047r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Client\Disallow Digest authentication
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Client
value_name: AllowDigest
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000520

SRG-OS-000125-GPOS-00065

SV-88263

The Windows Remote Management (WinRM) service must not use Basic authentication.

The Windows Remote Management (WinRM) service must not use Basic authentication.

Description

VulnDiscussion

Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential.

Documentable

false

F-80049r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> “Allow Basic authentication” to “Disabled”.

F-80049r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Service\Allow Basic authentication
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Service
value_name: AllowBasic
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000530

SRG-OS-000393-GPOS-00173

SV-88265

The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

Description

VulnDiscussion

Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.

Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Documentable

false

F-80051r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> “Allow unencrypted traffic” to “Disabled”.

F-80051r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Service
value_name: AllowUnencryptedTraffic
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-CC-000540

SRG-OS-000373-GPOS-00157

SV-88267

The Windows Remote Management (WinRM) service must not store RunAs credentials.

The Windows Remote Management (WinRM) service must not store RunAs credentials.

Description

VulnDiscussion

Storage of administrative credentials could allow unauthorized access. Disallowing the storage of RunAs credentials for Windows Remote Management will prevent them from being used with plug-ins.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80053r1 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> “Disallow WinRM from storing RunAs credentials” to “Enabled”.

F-80053r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Windows Components\Windows
  Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Microsoft\Windows\WinRM\Service
value_name: DisableRunAs
action: DWORD:1
```

Version History

Version ‘r1’: created

WN16-CC-000550

SRG-OS-000066-GPOS-00034

SV-88269

The DoD Root CA certificates must be installed in the Trusted Root Store.

The DoD Root CA certificates must be installed in the Trusted Root Store.

Description

VulnDiscussion

To ensure secure DoD websites and DoD-signed code are properly validated, the system must trust the DoD Root Certificate Authorities (CAs). The DoD root certificates will ensure that the trust chain is established for server certificates issued from the DoD CAs.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Documentable

false

F-87311r1 Implementation Example

Install the DoD Root CA certificates:

DoD Root CA 2 DoD Root CA 3 DoD Root CA 4 DoD Root CA 5

The InstallRoot tool is available on IASE at http://iase.disa.mil/pki-pke/Pages/tools.aspx.

Version History

Version ‘r3’: created

WN16-PK-000010

SRG-OS-000066-GPOS-00034

SV-88271

The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Description

VulnDiscussion

To ensure users do not experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CAs, the DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificate Store. This requirement only applies to unclassified systems.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Documentable

false

F-87313r2 Implementation Example

Install the DoD Interoperability Root CA cross-certificates on unclassified systems.

Issued To - Issued By - Thumbprint DoD Root CA 2 - DoD Interoperability Root CA 1 - 22BBE981F0694D246CC1472ED2B021DC8540A22F

DoD Root CA 3 - DoD Interoperability Root CA 2 - FFAD03329B9E527A43EEC66A56F9CBB5393E6E13

DoD Root CA 3 - DoD Interoperability Root CA 2 - FCE1B1E25374DD94F5935BEB86CA643D8C8D1FF4

Administrators should run the Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool once as an administrator and once as the current user.

The FBCA Cross-Certificate Remover Tool and User Guide are available on IASE at http://iase.disa.mil/pki-pke/Pages/tools.aspx.

Version History

Version ‘r2’: created

WN16-PK-000020

SRG-OS-000066-GPOS-00034

SV-88273

The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Description

VulnDiscussion

To ensure users do not experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CAs, the US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificate Store. This requirement only applies to unclassified systems.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

Documentable

false

F-87315r1 Implementation Example

Install the US DoD CCEB Interoperability Root CA cross-certificate on unclassified systems.

Issued To - Issued By - Thumbprint DoD Root CA 2 - US DoD CCEB Interoperability Root CA 1 - DA36FAF56B2F6FBA1604F5BE46D864C9FA013BA3

DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 - 929BF3196896994C0A201DF4A5B71F603FEFBF2E

Administrators should run the Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool once as an administrator and once as the current user.

The FBCA Cross-Certificate Remover Tool and User Guide are available on IASE at http://iase.disa.mil/pki-pke/Pages/tools.aspx.

Version History

Version ‘r2’: created

WN16-PK-000030

SRG-OS-000480-GPOS-00227

SV-88285

Local accounts with blank passwords must be restricted to prevent access from the network.

Local accounts with blank passwords must be restricted to prevent access from the network.

Description

VulnDiscussion

An account without a password can allow unauthorized access to a system as only the username would be required. Password policies should prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password does exist, enabling this setting will prevent network access, limiting the account to local console logon only.

Documentable

false

F-80071r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Accounts: Limit local account use of blank passwords to console logon only” to “Enabled”.

F-80071r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000020

SRG-OS-000480-GPOS-00227

SV-88287

The built-in administrator account must be renamed.

The built-in administrator account must be renamed.

Description

VulnDiscussion

The built-in administrator account is a well-known account subject to attack. Renaming this account to an unidentified name improves the protection of this account and the system.

Documentable

false

F-80073r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Accounts: Rename administrator account” to a name other than “Administrator”.

F-80073r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Accounts: Rename administrator account'
value: Administrator
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: NewAdministratorName
section: System Access
value: '"Administrator"'
```

Version History

Version ‘r1’: created

WN16-SO-000030

SRG-OS-000480-GPOS-00227

SV-88289

The built-in guest account must be renamed.

The built-in guest account must be renamed.

Description

VulnDiscussion

The built-in guest account is a well-known user account on all Windows systems and, as initially installed, does not require a password. This can allow access to system resources by unauthorized users. Renaming this account to an unidentified name improves the protection of this account and the system.

Documentable

false

F-80075r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Accounts: Rename guest account” to a name other than “Guest”.

F-80075r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Accounts: Rename guest account'
value: Guest
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: NewGuestName
section: System Access
value: '"Guest"'
```

Version History

Version ‘r1’: created

WN16-SO-000040

SRG-OS-000062-GPOS-00031

SV-88291

Audit policy using subcategories must be enabled.

Audit policy using subcategories must be enabled.

Description

VulnDiscussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior. This setting allows administrators to enable more precise auditing capabilities.

Documentable

false

F-80077r1 Implementation Example

Configure the policy value for 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” to “Enabled”.

F-80077r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\SceNoApplyLegacyAuditPolicy
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000050

SRG-OS-000423-GPOS-00187

SV-88293

Domain controllers must require LDAP access signing.

Domain controllers must require LDAP access signing.

Description

VulnDiscussion

Unsigned network traffic is susceptible to man-in-the-middle attacks, where an intruder captures packets between the server and the client and modifies them before forwarding them to the client. In the case of an LDAP server, this means that an attacker could cause a client to make decisions based on false records from the LDAP directory. The risk of an attacker pulling this off can be decreased by implementing strong physical security measures to protect the network infrastructure. Furthermore, implementing Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for Internet Protocol (IP) traffic, can make all types of man-in-the-middle attacks extremely difficult.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80079r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain controller: LDAP server signing requirements” to “Require signing”.

F-80079r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity
section: Registry Values
value: '2'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-DC-000320

SRG-OS-000480-GPOS-00227

SV-88295

Domain controllers must be configured to allow reset of machine account passwords.

Domain controllers must be configured to allow reset of machine account passwords.

Description

VulnDiscussion

Enabling this setting on all domain controllers in a domain prevents domain members from changing their computer account passwords. If these passwords are weak or compromised, the inability to change them may leave these computers vulnerable.

Documentable

false

F-80081r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain controller: Refuse machine account password changes” to “Disabled”.

F-80081r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-DC-000330

SRG-OS-000423-GPOS-00187

SV-88297

The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.

The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.

Description

VulnDiscussion

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic will be encrypted and signed.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80083r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Digitally encrypt or sign secure channel data (always)” to “Enabled”.

F-80083r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000080

SRG-OS-000423-GPOS-00187

SV-88299

The setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.

The setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.

Description

VulnDiscussion

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but not all information is encrypted. If this policy is enabled, outgoing secure channel traffic will be encrypted.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80085r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Digitally encrypt secure channel data (when possible)” to “Enabled”.

F-80085r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000090

SRG-OS-000423-GPOS-00187

SV-88301

The setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.

The setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.

Description

VulnDiscussion

Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked. If this policy is enabled, outgoing secure channel traffic will be signed.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80087r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Digitally sign secure channel data (when possible)” to “Enabled”.

F-80087r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000100

SRG-OS-000379-GPOS-00164

SV-88303

The computer account password must not be prevented from being reset.

The computer account password must not be prevented from being reset.

Description

VulnDiscussion

Computer account passwords are changed automatically on a regular basis. Disabling automatic password changes can make the system more vulnerable to malicious access. Frequent password changes can be a significant safeguard for the system. A new password for the computer account will be generated every 30 days.

Documentable

false

F-80089r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Disable machine account password changes” to “Disabled”.

F-80089r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000110

SRG-OS-000480-GPOS-00227

SV-88305

The maximum age for machine account passwords must be configured to 30 days or less.

The maximum age for machine account passwords must be configured to 30 days or less.

Description

VulnDiscussion

Computer account passwords are changed automatically on a regular basis. This setting controls the maximum password age that a machine account may have. This must be set to no more than 30 days, ensuring the machine changes its password monthly.

Documentable

false

F-80091r1 Implementation Example

This is the default configuration for this setting (30 days).

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Maximum machine account password age” to “30” or less (excluding “0”, which is unacceptable).

F-80091r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Domain member: Maximum machine account password age'
value: 30
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge
section: Registry Values
value: 30
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000120

SRG-OS-000423-GPOS-00187

SV-88307

Windows Server 2016 must be configured to require a strong session key.

Windows Server 2016 must be configured to require a strong session key.

Description

VulnDiscussion

A computer connecting to a domain controller will establish a secure channel. The secure channel connection may be subject to compromise, such as hijacking or eavesdropping, if strong session keys are not used to establish the connection. Requiring strong session keys enforces 128-bit encryption between systems.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80093r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Domain member: Require strong (Windows 2000 or Later) session key” to “Enabled”.

F-80093r1 Machine readable information

Windows GPO Setting

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

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000130

SRG-OS-000029-GPOS-00010

SV-88309

The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.

The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.

Description

VulnDiscussion

Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer.

Documentable

false

F-80095r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Interactive logon: Machine inactivity limit” to “900” seconds or less, excluding “0” which is effectively disabled.

F-80095r2 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Interactive logon: Machine inactivity limit'
value: 900
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\InactivityTimeoutSecs
section: Registry Values
value: 900
type_value: 4
```

Version History

Version ‘r2’: created

WN16-SO-000140

SRG-OS-000023-GPOS-00006

SV-88311

The required legal notice must be configured to display before console logon.

The required legal notice must be configured to display before console logon.

Description

VulnDiscussion

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Documentable

false

F-80097r2 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Interactive Logon: Message text for users attempting to log on” to the following:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests–not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

F-80097r2 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Interactive logon: Message text for users attempting to
  log on'
value:
- You are accessing a U.S. Government (USG) Information System (IS) that is provided
  for USG-authorized use only.
- 'By using this IS (which includes any device attached to this IS), you consent to
  the following conditions:'
- The USG routinely intercepts and monitors communications on this IS for purposes
  including, but not limited to, penetration testing, COMSEC monitoring, network operations
  and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence
  (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to
  routine monitoring, interception, and search, and may be disclosed or used for any
  USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to
  protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or
  CI investigative searching or monitoring of the content of privileged communications,
  or work product, related to personal representation or services by attorneys, psychotherapists,
  or clergy, and their assistants. Such communications and work product are private
  and confidential. See User Agreement for details.
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\legalnoticetext
section: Registry Values
value:
- You are accessing a U.S. Government (USG) Information System (IS) that is provided
  for USG-authorized use only.
- 'By using this IS (which includes any device attached to this IS), you consent to
  the following conditions:'
- The USG routinely intercepts and monitors communications on this IS for purposes
  including, but not limited to, penetration testing, COMSEC monitoring, network operations
  and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence
  (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to
  routine monitoring, interception, and search, and may be disclosed or used for any
  USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to
  protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or
  CI investigative searching or monitoring of the content of privileged communications,
  or work product, related to personal representation or services by attorneys, psychotherapists,
  or clergy, and their assistants. Such communications and work product are private
  and confidential. See User Agreement for details.
type_value: 7
```

Version History

Version ‘r2’: created

WN16-SO-000150

SRG-OS-000023-GPOS-00006

SV-88313

The Windows dialog box title for the legal banner must be configured with the appropriate text.

The Windows dialog box title for the legal banner must be configured with the appropriate text.

Description

VulnDiscussion

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Documentable

false

F-80099r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Interactive Logon: Message title for users attempting to log on” to “DoD Notice and Consent Banner”, “US Department of Defense Warning Statement”, or an organization-defined equivalent.

If an organization-defined title is used, it can in no case contravene or modify the language of the message text required in WN16-SO-000150.

F-80099r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Interactive logon: Message title for users attempting
  to log on'
value: US Department of Defense Warning Statement
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\legalnoticecaption
section: Registry Values
value: US Department of Defense Warning Statement
type_value: 1
```

Version History

Version ‘r1’: created

WN16-SO-000160

SRG-OS-000480-GPOS-00227

SV-88315

Caching of logon credentials must be limited.

Caching of logon credentials must be limited.

Description

VulnDiscussion

The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons, such as the user's machine being disconnected from the network or domain controllers being unavailable. Even though the credential cache is well protected, if a system is attacked, an unauthorized individual may isolate the password to a domain user account using a password-cracking program and gain access to the domain.

Documentable

false

F-80271r1 Implementation Example

Configure the policy value for 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)" to "4" logons or less.

F-80271r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Interactive logon: Number of previous logons to cache
  (in case domain controller is not available)'
value: 4
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount
section: Registry Values
value: 4
type_value: 1
```

Version History

Version 'r1': created

WN16-MS-000050

SRG-OS-000423-GPOS-00187

SV-88317

The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

Description

VulnDiscussion

The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80103r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft network client: Digitally sign communications (always)” to “Enabled”.

F-80103r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network client: Digitally sign communications
  (always)'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000190

SRG-OS-000423-GPOS-00187

SV-88319

The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.

The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.

Description

VulnDiscussion

The server message block (SMB) protocol provides the basis for many network operations. If this policy is enabled, the SMB client will request packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80105r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft network client: Digitally sign communications (if server agrees)” to “Enabled”.

F-80105r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network client: Digitally sign communications
  (if server agrees)'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000200

SRG-OS-000074-GPOS-00042

SV-88321

Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.

Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.

Description

VulnDiscussion

Some non-Microsoft SMB servers only support unencrypted (plain-text) password authentication. Sending plain-text passwords across the network when authenticating to an SMB server reduces the overall security of the environment. Check with the vendor of the SMB server to determine if there is a way to support encrypted password authentication.

Documentable

false

F-80107r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft Network Client: Send unencrypted password to third-party SMB servers” to “Disabled”.

F-80107r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network client: Send unencrypted password to
  third-party SMB servers'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000210

SRG-OS-000163-GPOS-00072

SV-88323

The amount of idle time required before suspending a session must be configured to 15 minutes or less.

The amount of idle time required before suspending a session must be configured to 15 minutes or less.

Description

VulnDiscussion

Open sessions can increase the avenues of attack on a system. This setting is used to control when a computer disconnects an inactive SMB session. If client activity resumes, the session is automatically reestablished. This protects critical and sensitive network data from exposure to unauthorized personnel with physical access to the computer.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Documentable

false

F-80109r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft Network Server: Amount of idle time required before suspending session” to “15” minutes or less.

F-80109r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network server: Amount of idle time required
  before suspending session'
value: 15
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoDisconnect
section: Registry Values
value: 15
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000220

SRG-OS-000423-GPOS-00187

SV-88325

The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.

The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.

Description

VulnDiscussion

The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB server will only communicate with an SMB client that performs SMB packet signing.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80111r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft network server: Digitally sign communications (always)” to “Enabled”.

F-80111r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network server: Digitally sign communications
  (always)'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\RequireSecuritySignature
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000230

SRG-OS-000423-GPOS-00187

SV-88327

The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

Description

VulnDiscussion

The server message block (SMB) protocol provides the basis for many network operations. Digitally signed SMB packets aid in preventing man-in-the-middle attacks. If this policy is enabled, the SMB server will negotiate SMB packet signing as requested by the client.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188

Documentable

false

F-80113r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft network server: Digitally sign communications (if client agrees)” to “Enabled”.

F-80113r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Microsoft network server: Digitally sign communications
  (if client agrees)'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\EnableSecuritySignature
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000240

SRG-OS-000480-GPOS-00227

SV-88331

Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.

Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.

Description

VulnDiscussion

Anonymous enumeration of SAM accounts allows anonymous logon users (null session connections) to list all accounts names, thus providing a list of potential points to attack the system.

Documentable

false

F-80117r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network access: Do not allow anonymous enumeration of SAM accounts” to “Enabled”.

F-80117r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Do not allow anonymous enumeration of
  SAM accounts'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymousSam
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000260

SRG-OS-000138-GPOS-00069

SV-88333

Anonymous enumeration of shares must not be allowed.

Anonymous enumeration of shares must not be allowed.

Description

VulnDiscussion

Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system.

Documentable

false

F-80119r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network access: Do not allow anonymous enumeration of SAM accounts and shares” to “Enabled”.

F-80119r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Do not allow anonymous enumeration of
  SAM accounts and shares'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000270

SRG-OS-000373-GPOS-00157

SV-88335

Windows Server 2016 must be configured to prevent the storage of passwords and credentials.

Windows Server 2016 must be configured to prevent the storage of passwords and credentials.

Description

VulnDiscussion

This setting controls the storage of passwords and credentials for network authentication on the local system. Such credentials must not be stored on the local machine, as that may lead to account compromise.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80121r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network access: Do not allow storage of passwords and credentials for network authentication” to “Enabled”.

F-80121r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Do not allow storage of passwords and
  credentials for network authentication'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\DisableDomainCreds
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000280

SRG-OS-000480-GPOS-00227

SV-88337

Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.

Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.

Description

VulnDiscussion

Access by anonymous users must be restricted. If this setting is enabled, anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users must not have these permissions or rights.

Documentable

false

F-80123r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network access: Let everyone permissions apply to anonymous users” to “Disabled”.

F-80123r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Let Everyone permissions apply to anonymous
  users'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000290

SRG-OS-000138-GPOS-00069

SV-88339

Anonymous access to Named Pipes and Shares must be restricted.

Anonymous access to Named Pipes and Shares must be restricted.

Description

VulnDiscussion

Allowing anonymous access to named pipes or shares provides the potential for unauthorized system access. This setting restricts access to those defined in “Network access: Named Pipes that can be accessed anonymously” and “Network access: Shares that can be accessed anonymously”, both of which must be blank under other requirements.

Documentable

false

F-80125r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network access: Restrict anonymous access to Named Pipes and Shares” to “Enabled”.

F-80125r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Restrict anonymous access to Named Pipes
  and Shares'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RestrictNullSessAccess
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000300

SRG-OS-000324-GPOS-00125

SV-88341

Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

Description

VulnDiscussion

The Windows Security Account Manager (SAM) stores users' passwords. Restricting Remote Procedure Call (RPC) connections to the SAM to Administrators helps protect those credentials.

Documentable

false

F-80127r1 Implementation Example

Navigate to the policy Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Network access: Restrict clients allowed to make remote calls to SAM". Select "Edit Security" to configure the "Security descriptor:".

Add "Administrators" in "Group or user names:" if it is not already listed (this is the default).

Select "Administrators" in "Group or user names:".

Select "Allow" for "Remote Access" in "Permissions for"Administrators".

Click "OK".

The "Security descriptor:" must be populated with "O:BAG:BAD:(A;;RC;;;BA) for the policy to be enforced.

F-80127r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network access: Restrict clients allowed to make remote
  calls to SAM'
value: 'Administrators: Remote Access: Allow'
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam
section: Registry Values
value: O:BAG:BAD:(A;;RC;;;BA)
type_value: 1
```

Version History

Version 'r2': created

WN16-MS-000310

SRG-OS-000480-GPOS-00227

SV-88343

Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.

Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.

Description

VulnDiscussion

Services using Local System that use Negotiate when reverting to NTLM authentication may gain unauthorized access if allowed to authenticate anonymously versus using the computer identity.

Documentable

false

F-80129r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Allow Local System to use computer identity for NTLM” to “Enabled”.

F-80129r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Allow Local System to use computer identity
  for NTLM'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\UseMachineId
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000320

SRG-OS-000480-GPOS-00227

SV-88345

NTLM must be prevented from falling back to a Null session.

NTLM must be prevented from falling back to a Null session.

Description

VulnDiscussion

NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access.

Documentable

false

F-80131r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Allow LocalSystem NULL session fallback” to “Disabled”.

F-80131r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Allow LocalSystem NULL session fallback'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AllowNullSessionFallback
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000330

SRG-OS-000480-GPOS-00227

SV-88347

PKU2U authentication using online identities must be prevented.

PKU2U authentication using online identities must be prevented.

Description

VulnDiscussion

PKU2U is a peer-to-peer authentication protocol. This setting prevents online identities from authenticating to domain-joined systems. Authentication will be centrally managed with Windows user accounts.

Documentable

false

F-80133r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Allow PKU2U authentication requests to this computer to use online identities” to “Disabled”.

F-80133r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Allow PKU2U authentication requests
  to this computer to use online identities'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\pku2u\AllowOnlineID
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000340

SRG-OS-000120-GPOS-00061

SV-88349

Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

Description

VulnDiscussion

Certain encryption types are no longer considered secure. The DES and RC4 encryption suites must not be used for Kerberos encryption.

Documentable

false

F-80135r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Configure encryption types allowed for Kerberos” to “Enabled” with only the following selected:

AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types

F-80135r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Configure encryption types allowed for
  Kerberos'
value: AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionTypes
section: Registry Values
value: '2147483640'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000350

SRG-OS-000073-GPOS-00041

SV-88351

Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.

Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.

Description

VulnDiscussion

The LAN Manager hash uses a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords. This setting controls whether a LAN Manager hash of the password is stored in the SAM the next time the password is changed.

Documentable

false

F-80137r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Do not store LAN Manager hash value on next password change” to “Enabled”.

F-80137r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Do not store LAN Manager hash value
  on next password change'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000360

SRG-OS-000163-GPOS-00072

SV-88353

Windows Server 2016 must be configured to force users to log off when their allowed logon hours expire.

Windows Server 2016 must be configured to force users to log off when their allowed logon hours expire.

Description

VulnDiscussion

Limiting logon hours can help protect data by allowing access only during specified times. This setting controls whether users are forced to log off when their allowed logon hours expire. If logon hours are set for users, this must be enforced.

Documentable

false

F-80139r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Force logoff when logon hours expire” to “Enabled”.

F-80139r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Force logoff when logon hours expire'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000370

SRG-OS-000480-GPOS-00227

SV-88355

The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.

The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.

Description

VulnDiscussion

The Kerberos v5 authentication protocol is the default for authentication of users who are logging on to domain accounts. NTLM, which is less secure, is retained in later Windows versions for compatibility with clients and servers that are running earlier versions of Windows or applications that still use it. It is also used to authenticate logons to standalone computers that are running later versions.

Documentable

false

F-80141r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: LAN Manager authentication level” to “Send NTLMv2 response only. Refuse LM & NTLM”.

F-80141r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: LAN Manager authentication level'
value: Send NTLMv2 response only. Refuse LM & NTLM
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel
section: Registry Values
value: '5'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000380

SRG-OS-000480-GPOS-00227

SV-88357

Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.

Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.

Description

VulnDiscussion

This setting controls the signing requirements for LDAP clients. This must be set to “Negotiate signing” or “Require signing”, depending on the environment and type of LDAP server in use.

Documentable

false

F-80143r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: LDAP client signing requirements” to “Negotiate signing” at a minimum.

F-80143r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: LDAP client signing requirements'
value: Negotiate signing
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity
section: Registry Values
value: '1'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000390

SRG-OS-000480-GPOS-00227

SV-88359

Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.

Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.

Description

VulnDiscussion

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

Documentable

false

F-80145r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Minimum session security for NTLM SSP based (including secure RPC) clients” to “Require NTLMv2 session security” and “Require 128-bit encryption” (all options selected).

F-80145r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Minimum session security for NTLM SSP
  based (including secure RPC) clients'
value: Require NTLMv2 session security, Require 128-bit encryption
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec
section: Registry Values
value: '537395200'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000400

SRG-OS-000480-GPOS-00227

SV-88361

Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.

Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.

Description

VulnDiscussion

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

Documentable

false

F-80147r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Network security: Minimum session security for NTLM SSP based (including secure RPC) servers” to “Require NTLMv2 session security” and “Require 128-bit encryption” (all options selected).

F-80147r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Network security: Minimum session security for NTLM SSP
  based (including secure RPC) servers'
value: Require NTLMv2 session security, Require 128-bit encryption
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec
section: Registry Values
value: '537395200'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000410

SRG-OS-000067-GPOS-00035

SV-88363

Users must be required to enter a password to access private keys stored on the computer.

Users must be required to enter a password to access private keys stored on the computer.

Description

VulnDiscussion

If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Documentable

false

F-80149r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “System cryptography: Force strong key protection for user keys stored on the computer” to “User must enter a password each time they use a key”.

F-80149r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\System cryptography: Force strong key protection for user
  keys stored on the computer'
value: User must enter a password each time they use a key
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection
section: Registry Values
value: '2'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000420

SRG-OS-000033-GPOS-00014

SV-88365

Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

Description

VulnDiscussion

This setting ensures the system uses algorithms that are FIPS-compliant for encryption, hashing, and signing. FIPS-compliant algorithms meet specific standards established by the U.S. Government and must be the algorithms used for all OS encryption functions.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000478-GPOS-00223

Documentable

false

F-80151r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” to “Enabled”.

F-80151r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\System cryptography: Use FIPS compliant algorithms for
  encryption, hashing, and signing'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000430

SRG-OS-000480-GPOS-00227

SV-88367

Windows Server 2016 must be configured to require case insensitivity for non-Windows subsystems.

Windows Server 2016 must be configured to require case insensitivity for non-Windows subsystems.

Description

VulnDiscussion

This setting controls the behavior of non-Windows subsystems when dealing with the case of arguments or commands. Case sensitivity could lead to the access of files or commands that must be restricted. To prevent this from happening, case insensitivity restrictions must be required.

Documentable

false

F-80153r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “System objects: Require case insensitivity for non-Windows subsystems” to “Enabled”.

F-80153r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\System objects: Require case insensitivity for non-Windows
  subsystems'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000440

SRG-OS-000480-GPOS-00227

SV-88369

The default permissions of global system objects must be strengthened.

The default permissions of global system objects must be strengthened.

Description

VulnDiscussion

Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default Discretionary Access Control List (DACL) that specifies who can access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

Documentable

false

F-80155r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)” to “Enabled”.

F-80155r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\System objects: Strengthen default permissions of internal
  system objects (e.g., Symbolic Links) '
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000450

SRG-OS-000373-GPOS-00157

SV-88371

User Account Control approval mode for the built-in Administrator must be enabled.

User Account Control approval mode for the built-in Administrator must be enabled.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures the built-in Administrator account so that it runs in Admin Approval Mode.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80157r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Admin Approval Mode for the Built-in Administrator account” to “Enabled”.

F-80157r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Admin Approval Mode for the built-in
  Administrator account'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000460

SRG-OS-000134-GPOS-00068

SV-88373

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.

UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting prevents User Interface Accessibility programs from disabling the secure desktop for elevation prompts.

Documentable

false

F-80159r1 Implementation Example

Configure the policy value for 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” to “Disabled”.

F-80159r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Allow UIAccess applications to prompt
  for elevation without using the secure desktop'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableUIADesktopToggle
section: Registry Values
value: 0
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000470

SRG-OS-000134-GPOS-00068

SV-88375

User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.

User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures the elevation requirements for logged-on administrators to complete a task that requires raised privileges.

Documentable

false

F-80161r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode” to “Prompt for consent on the secure desktop”.

The more secure option for this setting, “Prompt for credentials on the secure desktop”, would also be acceptable.

F-80161r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Behavior of the elevation prompt
  for administrators in Admin Approval Mode'
value: Prompt for credentials on the secure desktop
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin
section: Registry Values
value: '1'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000480

SRG-OS-000373-GPOS-00157

SV-88377

User Account Control must automatically deny standard user requests for elevation.

User Account Control must automatically deny standard user requests for elevation.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting controls the behavior of elevation when requested by a standard user account.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80163r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Behavior of the elevation prompt for standard users” to “Automatically deny elevation requests”.

F-80163r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Behavior of the elevation prompt
  for standard users'
value: Automatically deny elevation requests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser
section: Registry Values
value: '0'
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000490

SRG-OS-000134-GPOS-00068

SV-88379

User Account Control must be configured to detect application installations and prompt for elevation.

User Account Control must be configured to detect application installations and prompt for elevation.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting requires Windows to respond to application installation requests by prompting for credentials.

Documentable

false

F-80165r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Detect application installations and prompt for elevation” to “Enabled”.

F-80165r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Detect application installations
  and prompt for elevation'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableInstallerDetection
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000500

SRG-OS-000134-GPOS-00068

SV-88381

User Account Control must only elevate UIAccess applications that are installed in secure locations.

User Account Control must only elevate UIAccess applications that are installed in secure locations.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures Windows to only allow applications installed in a secure location on the file system, such as the Program Files or the Windows32 folders, to run with elevated privileges.

Documentable

false

F-80167r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Only elevate UIAccess applications that are installed in secure locations” to “Enabled”.

F-80167r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Only elevate UIAccess applications
  that are installed in secure locations'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableSecureUIAPaths
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000510

SRG-OS-000373-GPOS-00157

SV-88383

User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.

Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156

Documentable

false

F-80169r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Run all administrators in Admin Approval Mode” to “Enabled”.

F-80169r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Run all administrators in Admin
  Approval Mode'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000520

SRG-OS-000134-GPOS-00068

SV-88385

User Account Control must virtualize file and registry write failures to per-user locations.

User Account Control must virtualize file and registry write failures to per-user locations.

Description

VulnDiscussion

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures non-UAC-compliant applications to run in virtualized file and registry entries in per-user locations, allowing them to run.

Documentable

false

F-80171r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “User Account Control: Virtualize file and registry write failures to per-user locations” to “Enabled”.

F-80171r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\User Account Control: Virtualize file and registry write
  failures to per-user locations'
value: Enabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableVirtualization
section: Registry Values
value: 1
type_value: 4
```

Version History

Version ‘r1’: created

WN16-SO-000530

SRG-OS-000324-GPOS-00125

SV-88393

The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.

The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Access Credential Manager as a trusted caller” user right may be able to retrieve the credentials of other accounts from Credential Manager.

Documentable

false

F-80179r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Access Credential Manager as a trusted caller” to be defined but containing no entries (blank).

F-80179r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Access Credential Manager as a trusted caller
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeTrustedCredManAccessPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-UR-000010

SRG-OS-000080-GPOS-00048

SV-88395

The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.

The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Access this computer from the network” right may access resources on the system, and this right must be limited to those requiring it.

Documentable

false

F-80181r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Access this computer from the network” to include only the following accounts or groups:

- Administrators
- Authenticated Users
- Enterprise Domain Controllers

F-80181r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Access this computer from the network
value:
- Administrators
- Authenticated Users
- Enterprise Domain Controllers
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeNetworkLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-544'
- '*S-1-5-11'
- '*S-1-5-9'
```

Version History

Version ‘r1’: created

WN16-DC-000340

SRG-OS-000080-GPOS-00048

SV-88397

The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.

The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Access this computer from the network” user right may access resources on the system, and this right must be limited to those requiring it.

Documentable

false

F-88221r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Access this computer from the network” to include only the following accounts or groups:

- Administrators
- Authenticated Users

F-88221r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Access this computer from the network
value:
- Administrators
- Authenticated Users
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeNetworkLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-544'
- '*S-1-5-11'
```

Version History

Version ‘r2’: created

WN16-MS-000340

SRG-OS-000324-GPOS-00125

SV-88399

The Act as part of the operating system user right must not be assigned to any groups or accounts.

The Act as part of the operating system user right must not be assigned to any groups or accounts.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Act as part of the operating system” user right can assume the identity of any user and gain access to resources that the user is authorized to access. Any accounts with this right can take complete control of a system.

Documentable

false

F-80185r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Act as part of the operating system” to be defined but containing no entries (blank).

F-80185r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Act as part of the operating system
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeTcbPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-UR-000030

SRG-OS-000324-GPOS-00125

SV-88401

The Add workstations to domain user right must only be assigned to the Administrators group.

The Add workstations to domain user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Add workstations to domain” right may add computers to a domain. This could result in unapproved or incorrectly configured systems being added to a domain.

Documentable

false

F-80187r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Add workstations to domain” to include only the following accounts or groups:

- Administrators

F-80187r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Add workstations to domain
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeMachineAccountPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-DC-000350

SRG-OS-000080-GPOS-00048

SV-88403

The Allow log on locally user right must only be assigned to the Administrators group.

The Allow log on locally user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Allow log on locally” user right can log on interactively to a system.

Documentable

false

F-80189r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Allow log on locally” to include only the following accounts or groups:

- Administrators

F-80189r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Allow log on locally
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000050

SRG-OS-000080-GPOS-00048

SV-88405

The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.

The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Allow log on through Remote Desktop Services” user right can access a system through Remote Desktop.

Documentable

false

F-80191r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Allow log on through Remote Desktop Services” to include only the following accounts or groups:

- Administrators

F-80191r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Allow log on through Remote Desktop Services
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeRemoteInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-DC-000360

SRG-OS-000324-GPOS-00125

SV-88407

The Back up files and directories user right must only be assigned to the Administrators group.

The Back up files and directories user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Back up files and directories” user right can circumvent file and directory permissions and could allow access to sensitive data.

Documentable

false

F-80193r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Back up files and directories” to include only the following accounts or groups:

- Administrators

F-80193r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Back up files and directories
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeBackupPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000070

SRG-OS-000324-GPOS-00125

SV-88409

The Create a pagefile user right must only be assigned to the Administrators group.

The Create a pagefile user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Create a pagefile” user right can change the size of a pagefile, which could affect system performance.

Documentable

false

F-80195r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Create a pagefile” to include only the following accounts or groups:

- Administrators

F-80195r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Create a pagefile
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeCreatePagefilePrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000080

SRG-OS-000324-GPOS-00125

SV-88411

The Create a token object user right must not be assigned to any groups or accounts.

The Create a token object user right must not be assigned to any groups or accounts.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Create a token object” user right allows a process to create an access token. This could be used to provide elevated rights and compromise a system.

Documentable

false

F-80197r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Create a token object” to be defined but containing no entries (blank).

F-80197r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Create a token object
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeCreateTokenPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-UR-000090

SRG-OS-000324-GPOS-00125

SV-88413

The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.

The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Create global objects” user right can create objects that are available to all sessions, which could affect processes in other users’ sessions.

Documentable

false

F-80199r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Create global objects” to include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

F-80199r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Create global objects
value:
- Administrators
- Service
- Local Service
- Network Service
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeCreateGlobalPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
- '*S-1-5-6'
- '*S-1-5-19'
- '*S-1-5-20'
```

Version History

Version ‘r1’: created

WN16-UR-000100

SRG-OS-000324-GPOS-00125

SV-88415

The Create permanent shared objects user right must not be assigned to any groups or accounts.

The Create permanent shared objects user right must not be assigned to any groups or accounts.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Create permanent shared objects” user right could expose sensitive data by creating shared objects.

Documentable

false

F-80201r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Create permanent shared objects” to be defined but containing no entries (blank).

F-80201r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Create permanent shared objects
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeCreatePermanentPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-UR-000110

SRG-OS-000324-GPOS-00125

SV-88417

The Create symbolic links user right must only be assigned to the Administrators group.

The Create symbolic links user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Create symbolic links” user right can create pointers to other objects, which could expose the system to attack.

Documentable

false

F-80203r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Create symbolic links” to include only the following accounts or groups:

- Administrators

Systems that have the Hyper-V role will also have “Virtual Machines” given this user right. If this needs to be added manually, enter it as “NT Virtual MachineMachines”.

F-80203r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Create symbolic links
value:
- Administrators
- NT Virtual Machine\Virtual Machines
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeCreateSymbolicLinkPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
- '*S-1-5-83-0'
```

Version History

Version ‘r1’: created

WN16-UR-000120

SRG-OS-000324-GPOS-00125

SV-88419

The Debug programs user right must only be assigned to the Administrators group.

The Debug programs user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Debug programs” user right can attach a debugger to any process or to the kernel, providing complete access to sensitive and critical operating system components. This right is given to Administrators in the default configuration.

Documentable

false

F-80205r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Debug programs” to include only the following accounts or groups:

- Administrators

F-80205r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Debug programs
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDebugPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000130

SRG-OS-000080-GPOS-00048

SV-88421

The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.

The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny access to this computer from the network” user right defines the accounts that are prevented from logging on from the network.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-80207r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny access to this computer from the network” to include the following:

- Guests Group

F-80207r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny access to this computer from the network
value:
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyNetworkLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-546'
```

Version History

Version ‘r1’: created

WN16-DC-000370

SRG-OS-000080-GPOS-00048

SV-88423

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.

The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny access to this computer from the network” user right defines the accounts that are prevented from logging on from the network.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-88223r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny access to this computer from the network” to include the following:

Domain Systems Only: - Enterprise Admins group - Domain Admins group - “Local account and member of Administrators group” or “Local account” (see Note below)

All Systems: - Guests group

Note: These are built-in security groups. “Local account” is more restrictive but may cause issues on servers such as systems that provide failover clustering.

F-88223r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny access to this computer from the network
value:
- Enterprise Admins
- Domain Admins
- Local account and member of Administrators group
- Local account
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyNetworkLogonRight
section: Privilege Rights
value:
- '*S-1-5-21root domain-519'
- '*S-1-5-21domain-512'
- '*S-1-5-114'
- '*S-1-5-113'
- '*S-1-5-32-546'
```

Version History

Version ‘r2’: created

WN16-MS-000370

SRG-OS-000080-GPOS-00048

SV-88425

The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.

The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on as a batch job” user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

The Guests group must be assigned to prevent unauthenticated access.

Documentable

false

F-80211r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on as a batch job” to include the following:

- Guests Group

F-80211r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on as a batch job
value:
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyBatchLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-546'
```

Version History

Version ‘r1’: created

WN16-DC-000380

SRG-OS-000080-GPOS-00048

SV-88427

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on as a batch job” user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

The Guests group must be assigned to prevent unauthenticated access.

Documentable

false

F-80213r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on as a batch job” to include the following:

Domain Systems Only: - Enterprise Admins Group - Domain Admins Group

All Systems: - Guests Group

F-80213r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on as a batch job
value:
- Enterprise Admins
- Domain Admins
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyBatchLogonRight
section: Privilege Rights
value:
- '*S-1-5-21root domain-519'
- '*S-1-5-21domain-512'
- '*S-1-5-32-546'
```

Version History

Version ‘r1’: created

WN16-MS-000380

SRG-OS-000080-GPOS-00048

SV-88429

The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.

The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on as a service” user right defines accounts that are denied logon as a service.

Incorrect configurations could prevent services from starting and result in a denial of service.

Documentable

false

F-80215r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on as a service” to include no entries (blank).

F-80215r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on as a service
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyServiceLogonRight
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-DC-000390

SRG-OS-000080-GPOS-00048

SV-88431

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.

The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on as a service” user right defines accounts that are denied logon as a service.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

Incorrect configurations could prevent services from starting and result in a DoS.

Documentable

false

F-80217r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on as a service” to include the following:

Domain systems: - Enterprise Admins Group - Domain Admins Group

F-80217r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on as a service
value:
- Enterprise Admins
- Domain Admins
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyServiceLogonRight
section: Privilege Rights
value:
- '*S-1-5-21root domain-519'
- '*S-1-5-21domain-512'
```

Version History

Version ‘r1’: created

WN16-MS-000390

SRG-OS-000080-GPOS-00048

SV-88433

The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.

The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on locally” user right defines accounts that are prevented from logging on interactively.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-80219r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on locally” to include the following:

- Guests Group

F-80219r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on locally
value:
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-546'
```

Version History

Version ‘r1’: created

WN16-DC-000400

SRG-OS-000080-GPOS-00048

SV-88435

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on locally” user right defines accounts that are prevented from logging on interactively.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-88225r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on locally” to include the following:

Domain Systems Only: - Enterprise Admins Group - Domain Admins Group

All Systems: - Guests Group

F-88225r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on locally
value:
- Enterprise Admins
- Domain Admins
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-21root domain-519'
- '*S-1-5-21domain-512'
- '*S-1-5-32-546'
```

Version History

Version ‘r2’: created

WN16-MS-000400

SRG-OS-000297-GPOS-00115

SV-88437

The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.

The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on through Remote Desktop Services” user right defines the accounts that are prevented from logging on using Remote Desktop Services.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-80223r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on through Remote Desktop Services” to include the following:

- Guests Group

F-80223r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on through Remote Desktop Services
value:
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyRemoteInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-32-546'
```

Version History

Version ‘r1’: created

WN16-DC-000410

SRG-OS-000297-GPOS-00115

SV-88439

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.

The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Deny log on through Remote Desktop Services” user right defines the accounts that are prevented from logging on using Remote Desktop Services.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.

The Guests group must be assigned this right to prevent unauthenticated access.

Documentable

false

F-88227r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Deny log on through Remote Desktop Services” to include the following:

Domain Systems Only: - Enterprise Admins group - Domain Admins group - Local account (see Note below)

All Systems: - Guests group

Note: “Local account” is referring to the Windows built-in security group.

F-88227r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Deny log on through Remote Desktop Services
value:
- Enterprise Admins
- Domain Admins
- Local account
- Guests
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeDenyRemoteInteractiveLogonRight
section: Privilege Rights
value:
- '*S-1-5-21root domain-519'
- '*S-1-5-21domain-512'
- '*S-1-5-113'
- '*S-1-5-32-546'
```

Version History

Version ‘r2’: created

WN16-MS-000410

SRG-OS-000324-GPOS-00125

SV-88441

The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.

The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Enable computer and user accounts to be trusted for delegation” user right allows the “Trusted for Delegation” setting to be changed. This could allow unauthorized users to impersonate other users.

Documentable

false

F-80227r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Enable computer and user accounts to be trusted for delegation” to include only the following accounts or groups:

- Administrators

F-80227r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Enable computer and user accounts to be trusted
  for delegation
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeEnableDelegationPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-DC-000420

SRG-OS-000324-GPOS-00125

SV-88443

The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.

The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Enable computer and user accounts to be trusted for delegation” user right allows the “Trusted for Delegation” setting to be changed. This could allow unauthorized users to impersonate other users.

Documentable

false

F-80229r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Enable computer and user accounts to be trusted for delegation” to be defined but containing no entries (blank).

F-80229r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Enable computer and user accounts to be trusted
  for delegation
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeEnableDelegationPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-MS-000420

SRG-OS-000324-GPOS-00125

SV-88445

The Force shutdown from a remote system user right must only be assigned to the Administrators group.

The Force shutdown from a remote system user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Force shutdown from a remote system” user right can remotely shut down a system, which could result in a denial of service.

Documentable

false

F-80231r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Force shutdown from a remote system” to include only the following accounts or groups:

- Administrators

F-80231r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Force shutdown from a remote system
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeRemoteShutdownPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000200

SRG-OS-000324-GPOS-00125

SV-88447

The Generate security audits user right must only be assigned to Local Service and Network Service.

The Generate security audits user right must only be assigned to Local Service and Network Service.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Generate security audits” user right specifies users and processes that can generate Security Log audit records, which must only be the system service accounts defined.

Documentable

false

F-80233r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Generate security audits” to include only the following accounts or groups:

- Local Service
- Network Service

F-80233r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Generate security audits
value:
- Local Service
- Network Service
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeAuditPrivilege
section: Privilege Rights
value:
- '*S-1-5-19'
- '*S-1-5-20'
```

Version History

Version ‘r1’: created

WN16-UR-000210

SRG-OS-000324-GPOS-00125

SV-88449

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.

The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Impersonate a client after authentication” user right allows a program to impersonate another user or account to run on their behalf. An attacker could use this to elevate privileges.

Documentable

false

F-80235r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Impersonate a client after authentication” to include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

F-80235r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Impersonate a client after authentication
value:
- Administrators
- Service
- Local Service
- Network Service
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeImpersonatePrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
- '*S-1-5-6'
- '*S-1-5-19'
- '*S-1-5-20'
```

Version History

Version ‘r1’: created

WN16-UR-000220

SRG-OS-000324-GPOS-00125

SV-88451

The Increase scheduling priority user right must only be assigned to the Administrators group.

The Increase scheduling priority user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Increase scheduling priority” user right can change a scheduling priority, causing performance issues or a denial of service.

Documentable

false

F-80237r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Increase scheduling priority” to include only the following accounts or groups:

- Administrators

F-80237r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Increase scheduling priority
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeIncreaseBasePriorityPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000230

SRG-OS-000324-GPOS-00125

SV-88453

The Load and unload device drivers user right must only be assigned to the Administrators group.

The Load and unload device drivers user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Load and unload device drivers” user right allows a user to load device drivers dynamically on a system. This could be used by an attacker to install malicious code.

Documentable

false

F-80239r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Load and unload device drivers” to include only the following accounts or groups:

- Administrators

F-80239r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Load and unload device drivers
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeLoadDriverPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000240

SRG-OS-000324-GPOS-00125

SV-88455

The Lock pages in memory user right must not be assigned to any groups or accounts.

The Lock pages in memory user right must not be assigned to any groups or accounts.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The “Lock pages in memory” user right allows physical memory to be assigned to processes, which could cause performance issues or a denial of service.

Documentable

false

F-80241r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Lock pages in memory” to be defined but containing no entries (blank).

F-80241r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Lock pages in memory
value: []
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeLockMemoryPrivilege
section: Privilege Rights
value: []
```

Version History

Version ‘r1’: created

WN16-UR-000250

SRG-OS-000057-GPOS-00027

SV-88457

The Manage auditing and security log user right must only be assigned to the Administrators group.

The Manage auditing and security log user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Manage auditing and security log” user right can manage the security log and change auditing configurations. This could be used to clear evidence of tampering.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000063-GPOS-00032, SRG-OS-000337-GPOS-00129

Documentable

false

F-80243r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Manage auditing and security log” to include only the following accounts or groups:

- Administrators

F-80243r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Manage auditing and security log
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeSecurityPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000260

SRG-OS-000324-GPOS-00125

SV-88459

The Modify firmware environment values user right must only be assigned to the Administrators group.

The Modify firmware environment values user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Modify firmware environment values” user right can change hardware configuration environment variables. This could result in hardware failures or a denial of service.

Documentable

false

F-80245r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Modify firmware environment values” to include only the following accounts or groups:

- Administrators

F-80245r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Modify firmware environment values
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeSystemEnvironmentPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000270

SRG-OS-000324-GPOS-00125

SV-88461

The Perform volume maintenance tasks user right must only be assigned to the Administrators group.

The Perform volume maintenance tasks user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Perform volume maintenance tasks” user right can manage volume and disk configurations. This could be used to delete volumes, resulting in data loss or a denial of service.

Documentable

false

F-80247r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Perform volume maintenance tasks” to include only the following accounts or groups:

- Administrators

F-80247r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Perform volume maintenance tasks
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeManageVolumePrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000280

SRG-OS-000324-GPOS-00125

SV-88463

The Profile single process user right must only be assigned to the Administrators group.

The Profile single process user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Profile single process” user right can monitor non-system processes performance. An attacker could use this to identify processes to attack.

Documentable

false

F-80249r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Profile single process” to include only the following accounts or groups:

- Administrators

F-80249r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Profile single process
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeProfileSingleProcessPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000290

SRG-OS-000324-GPOS-00125

SV-88465

The Restore files and directories user right must only be assigned to the Administrators group.

The Restore files and directories user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Restore files and directories” user right can circumvent file and directory permissions and could allow access to sensitive data. It could also be used to overwrite more current data.

Documentable

false

F-80251r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Restore files and directories” to include only the following accounts or groups:

- Administrators

F-80251r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Restore files and directories
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeRestorePrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000300

SRG-OS-000324-GPOS-00125

SV-88467

The Take ownership of files or other objects user right must only be assigned to the Administrators group.

The Take ownership of files or other objects user right must only be assigned to the Administrators group.

Description

VulnDiscussion

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

Accounts with the “Take ownership of files or other objects” user right can take ownership of objects and make changes.

Documentable

false

F-80253r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> “Take ownership of files or other objects” to include only the following accounts or groups:

- Administrators

F-80253r1 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\User Rights Assignment\Take ownership of files and other objects
value:
- Administrators
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: SeTakeOwnershipPrivilege
section: Privilege Rights
value:
- '*S-1-5-32-544'
```

Version History

Version ‘r1’: created

WN16-UR-000310

SRG-OS-000480-GPOS-00227

SV-88473

The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Description

VulnDiscussion

Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended.

Documentable

false

F-80265r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Interactive logon: Smart card removal behavior” to “Lock Workstation” or “Force Logoff”.

F-80265r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Interactive logon: Smart card removal behavior'
value: Force Logoff
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption
section: Registry Values
value: '2'
type_value: 1
```

Version History

Version ‘r1’: created

WN16-SO-000180

SRG-OS-000121-GPOS-000062

SV-88475

The built-in guest account must be disabled.

The built-in guest account must be disabled.

Description

VulnDiscussion

A system faces an increased vulnerability threat if the built-in guest account is not disabled. This is a known account that exists on all Windows systems and cannot be deleted. This account is initialized during the installation of the operating system with no password assigned.

Documentable

false

F-80267r1 Implementation Example

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Accounts: Guest account status” to “Disabled”.

F-80267r1 Machine readable information

Windows GPO Setting

```
ui_path: 'Computer Configuration\Policies\Windows Settings\Security Settings\Local
  Policies\Security Options\Accounts: Guest account status'
value: Disabled
```

Windows INF-File (secedit.exe) Configuration

```
system: org.scapolite.implementation.win_secedit
setting_name: EnableGuestAccount
section: System Access
value: 0
```

Version History

Version ‘r1’: created

WN16-SO-000010

SRG-OS-000095-GPOS-00049

SV-92829

The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

Description

VulnDiscussion

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.

Documentable

false

F-84845r2 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> “Configure SMBv1 Server” to “Disabled”.

The system must be restarted for the change to take effect.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package. “SecGuide.admx” and “SecGuide.adml” must be copied to the and -US directories respectively.

F-84845r2 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\MS Security Guide\Configure
  SMB v1 server
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
value_name: SMB1
action: DWORD:0
```

Version History

Version ‘r1’: created

WN16-00-000411

SRG-OS-000095-GPOS-00049

SV-92831

The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

Description

VulnDiscussion

SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.

Documentable

false

F-84847r2 Implementation Example

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> “Configure SMBv1 client driver” to “Enabled” with “Disable driver (recommended)” selected for “Configure MrxSmb10 driver”.

The system must be restarted for the changes to take effect.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package. “SecGuide.admx” and “SecGuide.adml” must be copied to the and -US directories respectively.

F-84847r2 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\MS Security Guide\Configure
  SMB v1 client driver
value: Disable driver
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: SYSTEM\CurrentControlSet\Services\MrxSmb10
value_name: Start
action: DWORD:4
```

Version History

Version ‘r1’: created

WN16-00-000412

References