# Non-Compliance Report - Microsoft Windows Server 2016 STIG SCAP Benchmark

SCAP Compliance Checker - 5.7.1



## Score

# 44.57%

Adjusted Score: 44.57%
Original Score: 44.57%
**Compliance Status: RED**

| | | | |
|---|---|---|---|
| Pass: | 78 | Not Applicable: | 25 |
| Fail: | 97 | Not Checked: | 0 |
| Error: | 0 | Not Selected: | 0 |
| Unknown: | 0 | Informational: | 0 |
| Fixed: | 0 | Total: | 200 |

| | |
|---|---|
| BLUE: | Score equals 100 |
| GREEN: | Score is greater than or equal to 90 |
| YELLOW: | Score is greater than or equal to 80 |
| RED: | Score is greater than or equal to 0 |

## System Information

| | |
|---|---|
| Target Hostname: | WIN-4FBN6UUD6B0 |
| Operating System: | Microsoft Windows Server 2016 Datacenter Evaluation |
| OS Version: | 1607 |
| Domain: | |
| FQDN: | WIN-4FBN6UUD6B0. |
| Processor: | Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz |
| Processor Architecture: | Intel64 Family 6 Model 142 Stepping 9 |
| Processor Speed: | 2712 mhz |
| Physical Memory: | 0 mb |
| Manufacturer: | innotek GmbH |
| Model: | VirtualBox |
| Serial Number: | 0 |
| BIOS Version: | VirtualBox |
| Interfaces: | • [00000001] Intel(R) PRO/1000 MT Desktop Adapter<br>◦ IP Addresses<br>▪ 10.0.2.15<br>◦ MAC Address: 08:00:27:BC:7B:52 |

## Content Information

| | |
|---|---|
| Stream: | Windows_Server_2016_STIG |
| Profile: | Id: MAC-1_Classified |
| Digital Signature Status: | NOT DIGITALLY SIGNED |
| Stream Installation Date: | 2023-06-03 |
| Status: | accepted (2023-03-02) |
| Title: | Microsoft Windows Server 2016 STIG SCAP Benchmark |
| Description: | 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. |
| Notice: | |
| Front-Matter: | |
| Target Platforms: | • xccdf_mil.disa.stig_platform_Windows_Server_2016_Standalone |
| Reference: | Href: https://cyber.mil<br>Publisher: DISA<br>Source: STIG.DOD.MIL |

| | |
|---|---|
| Stream Version: | 002.004 |
| Source OVAL Version: | 5.10 |
| Result OVAL Version: | 5.11.2 |
| Source OCIL Version: | 0 |
| Result OCIL Version: | 0 |
| Start Time: | 2023-06-03T10:58:59 |
| End Time: | 2023-06-03T10:59:28 |
| Scanner: | cpe:/a:niwc:scc:5.7.1 |
| Identity: | WIN-4FBN6UUD6B0\Administrator |
| Identity Privileged: | true |
| Identity Authenticated: | true |
| Release Info: | Release: 2.4 Benchmark Date: 11 May 2023 |

# Detailed Results: High Severity (CAT I)

- V-224932 - AutoPlay must be turned off for non-volume devices. - (CCE-46805-8) - Fail
- V-224933 - The default AutoRun behavior must be configured to prevent AutoRun commands. - (CCE-46760-5) - Fail
- V-224934 - AutoPlay must be disabled for all drives. - (CCE-46970-0) - Fail
- V-224954 - The Windows Installer Always install with elevated privileges option must be disabled. - (CCE-47225-8) - Fail
- V-224958 - The Windows Remote Management (WinRM) client must not use Basic authentication. - (CCE-46295-2) - Fail
- V-224961 - The Windows Remote Management (WinRM) service must not use Basic authentication. - (CCE-45061-9) - Fail
- V-225046 - Anonymous enumeration of shares must not be allowed. - (CCE-46305-9) - Fail
- V-225054 - The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM. - (CCE-46565-8) - Fail

# Detailed Results: Medium Severity (CAT II)

- V-224856 - The Server Message Block (SMB) v1 protocol must be uninstalled. - Fail
- V-224857 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server. - Fail
- V-224858 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client. - Fail
- V-224866 - Windows 2016 account lockout duration must be configured to 15 minutes or greater. - (CCE-47152-4) - Fail
- V-224867 - Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less. - (CCE-46497-4) - Fail
- V-224868 - Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater. - (CCE-47272-0) - Fail
- V-224869 - Windows Server 2016 password history must be configured to 24 passwords remembered. - (CCE-44479-4) - Fail
- V-224871 - Windows Server 2016 minimum password age must be configured to at least one day. - (CCE-45608-7) - Fail
- V-224872 - Windows Server 2016 minimum password length must be configured to 14 characters. - Fail
- V-224882 - Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures. - (CCE-44732-6) - Fail
- V-224883 - Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes. - (CCE-45973-5) - Fail
- V-224886 - Windows Server 2016 must be configured to audit Account Management - User Account Management failures. - (CCE-46552-6) - Fail
- V-224888 - Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes. - (CCE-46177-2) - Fail
- V-224890 - Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures. - Fail
- V-224896 - Windows 2016 must be configured to audit Object Access - Other Object Access Events successes. - (CCE-45980-0) - Fail
- V-224897 - Windows 2016 must be configured to audit Object Access - Other Object Access Events failures. - (CCE-45980-0) - Fail
- V-224901 - Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures. - (CCE-45966-9) - Fail
- V-224903 - Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes. - (CCE-46306-7) - Fail
- V-224904 - Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes. - (CCE-45981-8) - Fail
- V-224905 - Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures. - (CCE-45981-8) - Fail
- V-224906 - Windows Server 2016 must be configured to audit System - IPsec Driver successes. - (CCE-46482-6) - Fail
- V-224907 - Windows Server 2016 must be configured to audit System - IPsec Driver failures. - (CCE-46482-6) - Fail
- V-224911 - Windows Server 2016 must be configured to audit System - Security System Extension successes. - (CCE-47111-0) - Fail
- V-224914 - The display of slide shows on the lock screen must be disabled. - Fail
- V-224915 - WDigest Authentication must be disabled on Windows Server 2016. - Fail
- V-224920 - Insecure logons to an SMB server must be disabled. - Fail
- V-224922 - Command line data must be included in process creation events. - (CCE-45411-6) - Fail
- V-224925 - Group Policy objects must be reprocessed even if they have not changed. - (CCE-46343-0) - Fail
- V-224926 - Downloading print driver packages over HTTP must be prevented. - (CCE-47107-8) - Fail
- V-224927 - Printing over HTTP must be prevented. - (CCE-47297-7) - Fail
- V-224928 - The network selection user interface (UI) must not be displayed on the logon screen. - Fail
- V-224929 - Users must be prompted to authenticate when the system wakes from sleep (on battery). - (CCE-47317-3) - Fail
- V-224930 - Users must be prompted to authenticate when the system wakes from sleep (plugged in). - (CCE-46919-7) - Fail
- V-224935 - Administrator accounts must not be enumerated during elevation. - (CCE-46465-1) - Fail
- V-224936 - Windows Telemetry must be configured to Security or Basic. - Fail
- V-224937 - The Application event log size must be configured to 32768 KB or greater. - (CCE-44494-3) - Fail
- V-224938 - The Security event log size must be configured to 196608 KB or greater. - (CCE-44526-2) - Fail
- V-224939 - The System event log size must be configured to 32768 KB or greater. - (CCE-46651-6) - Fail
- V-224940 - Windows Server 2016 Windows SmartScreen must be enabled. - (CCE-44884-5) - Fail
- V-224944 - Passwords must not be saved in the Remote Desktop Client. - (CCE-44880-3) - Fail
- V-224945 - Local drives must be prevented from sharing with Remote Desktop Session Hosts. - (CCE-46771-2) - Fail
- V-224946 - Remote Desktop Services must always prompt a client for passwords upon connection. - (CCE-45743-2) - Fail
- V-224947 - The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications. - (CCE-44496-8) - Fail
- V-224948 - Remote Desktop Services must be configured with the client connection encryption set to High Level. - (CCE-47193-8) - Fail
- V-224949 - Attachments must be prevented from being downloaded from RSS feeds. - (CCE-45063-5) - Fail
- V-224952 - Indexing of encrypted files must be turned off. - Fail
- V-224953 - Users must be prevented from changing installation options. - (CCE-46993-2) - Fail
- V-224957 - PowerShell script block logging must be enabled. - Fail
- V-224959 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic. - (CCE-46378-6) - Fail
- V-224960 - The Windows Remote Management (WinRM) client must not use Digest authentication. - (CCE-46014-7) - Fail
- V-224962 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic. - (CCE-45060-1) - Fail
- V-224963 - The Windows Remote Management (WinRM) service must not store RunAs credentials. - (CCE-46708-4) - Fail
- V-225010 - Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server. - (CCE-46880-1) - Fail
- V-225013 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators. - (CCE-45487-6) - Fail
- V-225014 - The "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on member servers. - (CCE-45486-8) - Fail

- V-225015 - 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. - (CCE-44499-2) - Fail
- V-225016 - 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. - (CCE-47287-8) - Fail
- V-225018 - 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. - (CCE-46108-7) - Fail
- V-225019 - 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. - (CCE-47279-5) - Fail
- V-225021 - The DoD Root CA certificates must be installed in the Trusted Root Store. - Fail
- V-225022 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems. - Fail
- V-225023 - The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems. - Fail
- V-225026 - Windows Server 2016 built-in administrator account must be renamed. - (CCE-46321-6) - Fail
- V-225027 - Windows Server 2016 built-in guest account must be renamed. - (CCE-46218-4) - Fail
- V-225028 - Audit policy using subcategories must be enabled. - (CCE-46406-5) - Fail
- V-225035 - The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver. - Fail
- V-225038 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation. - (CCE-46148-3) - Fail
- V-225039 - The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled. - (CCE-46135-0) - Fail
- V-225042 - The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled. - (CCE-47038-5) - Fail
- V-225043 - The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled. - (CCE-46230-9) - Fail
- V-225049 - Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously. - (CCE-46338-0) - Fail
- V-225050 - NTLM must be prevented from falling back to a Null session. - (CCE-47296-9) - Fail
- V-225051 - PKU2U authentication using online identities must be prevented. - (CCE-46030-3) - Fail
- V-225052 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites. - (CCE-44602-1) - Fail
- V-225056 - Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption. - (CCE-44861-3) - Fail
- V-225057 - Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption. - (CCE-46160-8) - Fail
- V-225058 - Users must be required to enter a password to access private keys stored on the computer. - (CCE-46878-5) - Fail
- V-225059 - Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing. - (CCE-44610-4) - Fail
- V-225061 - User Account Control approval mode for the built-in Administrator must be enabled. - (CCE-47000-5) - Fail
- V-225063 - User Account Control must, at a minimum, prompt administrators for consent on the secure desktop. - (CCE-47284-5) - Fail
- V-225064 - User Account Control must automatically deny standard user requests for elevation. - (CCE-47214-2) - Fail
- V-225072 - The Allow log on locally user right must only be assigned to the Administrators group. - (CCE-45723-4) - Fail
- V-225073 - The Back up files and directories user right must only be assigned to the Administrators group. - (CCE-44987-6) - Fail
- V-225092 - The Restore files and directories user right must only be assigned to the Administrators group. - (CCE-46176-4) - Fail

# Detailed Results: Low Severity (CAT III)

- V-224916 - Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing. - (CCE-45275-5) - Fail
- V-224917 - Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing. - (CCE-45276-3) - Fail
- V-224918 - Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes. - (CCE-45279-7) - Fail
- V-224919 - Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers. - (CCE-45283-9) - Fail
- V-224931 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft. - (CCE-45945-3) - Fail

# Detailed Results: High Severity (CAT I)

### V-224932 - AutoPlay must be turned off for non-volume devices.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224932r852325_rule |
| Result: | Fail |
| Version: | WN16-CC-000250 |
| Identities: | CCE-46805-8<br>SV-88209<br>V-73545<br>CCI-001764 (NIST SP 800-53 Rev 4: CM-7 (2); NIST SP 800-53 Rev 5: CM-7 (2)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> "Disallow Autoplay for non-volume devices" to "Enabled". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1097<br>Result: false<br>Title: WN16-CC-000250<br>Description: Autoplay must be turned off for non-volume devices.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Disallow Autoplay for non-volume devices' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109700 (registry_test)<br>Result: false<br>Title: 'Disallow Autoplay for non-volume devices' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\Explorer'<br>◦ name must be equal to 'NoAutoplayfornonVolume'<br>State ID: oval:mil.disa.stig.windows:ste:109700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224933 - The default AutoRun behavior must be configured to prevent AutoRun commands.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224933r852326_rule |
| Result: | Fail |
| Version: | WN16-CC-000260 |
| Identities: | CCE-46760-5<br>SV-88211<br>V-73547<br>CCI-001764 (NIST SP 800-53 Rev 4: CM-7 (2); NIST SP 800-53 Rev 5: CM-7 (2)) |
| Description: | Allowing AutoRun commands to execute may introduce malicious code to a system. Configuring this setting prevents AutoRun commands from executing. false |
| Fix Text: | 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. |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1098<br>Result: false<br>Title: WN16-CC-000260<br>Description: The default autorun behavior must be configured to prevent autorun commands.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Default behavior for AutoRun' is set to 'Enabled' with 'Do not execute any autorun commands' selected) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109800 (registry_test)<br>Result: false<br>Title: 'Default behavior for AutoRun' is set to 'Enabled' with 'Do not execute any autorun commands' selected<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109800 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\Explorer'<br>◦ name must be equal to 'NoAutorun'<br>State ID: oval:mil.disa.stig.windows:ste:109800 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224934 - AutoPlay must be disabled for all drives.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224934r852327_rule |
| Result: | Fail |
| Version: | WN16-CC-000270 |
| Identities: | CCE-46970-0<br>SV-88213<br>V-73549<br>CCI-001764 (NIST SP 800-53 Rev 4: CM-7 (2); NIST SP 800-53 Rev 5: CM-7 (2)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> "Turn off AutoPlay" to "Enabled" with "All Drives" selected. |
| Severity: | high |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1099<br>Result: false<br>Title: WN16-CC-000270<br>Description: Autoplay must be disabled for all drives.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Turn off AutoPlay' is set to 'Enabled' with 'All Drives' selected) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109900 (registry_test)<br>Result: false<br>Title: 'Turn off AutoPlay' is set to 'Enabled' with 'All Drives' selected<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109900 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer'<br>◦ name must be equal to 'NoDriveTypeAutoRun'<br>State ID: oval:mil.disa.stig.windows:ste:109900 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '255'<br>Additional Information: Check existence requirement not met. |

## V-224954 - The Windows Installer Always install with elevated privileges option must be disabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224954r852335_rule |
| Result: | Fail |
| Version: | WN16-CC-000460 |
| Identities: | CCE-47225-8<br>SV-88249<br>V-73585<br>CCI-001812 (NIST SP 800-53 Rev 4: CM-11 (2)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Always install with elevated privileges" to "Disabled". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1120<br>Result: false<br>Title: WN16-CC-000460<br>Description: The Windows Installer Always install with elevated privileges must be disabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Always install with elevated privileges' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112000 (registry_test)<br>Result: false<br>Title: 'Always install with elevated privileges' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112000 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\Installer'<br>◦ name must be equal to 'AlwaysInstallElevated'<br>State ID: oval:mil.disa.stig.windows:ste:112000 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224958 - The Windows Remote Management (WinRM) client must not use Basic authentication.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224958r877395_rule |
| Result: | Fail |
| Version: | WN16-CC-000500 |

| | |
|---|---|
| Identities: | CCE-46295-2<br>V-73593<br>SV-88257<br>CCI-000877 (NIST SP 800-53: MA-4 c; NIST SP 800-53A: MA-4.1 (iv); NIST SP 800-53 Rev 4: MA-4 c; NIST SP 800-53 Rev 5: MA-4 c) |
| Description: | Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> "Allow Basic authentication" to "Disabled". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1123<br>Result: false<br>Title: WN16-CC-000500<br>Description: The Windows Remote Management (WinRM) client must not use Basic authentication.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Allow Basic authentication' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112300 (registry_test)<br>Result: false<br>Title: 'Allow Basic authentication' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Client'<br>◦ name must be equal to 'AllowBasic'<br>State ID: oval:mil.disa.stig.windows:ste:112300 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

### V-224961 - The Windows Remote Management (WinRM) service must not use Basic authentication.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224961r877395_rule |
| Result: | Fail |
| Version: | WN16-CC-000530 |
| Identities: | CCE-45061-9<br>SV-88263<br>V-73599<br>CCI-000877 (NIST SP 800-53: MA-4 c; NIST SP 800-53A: MA-4.1 (iv); NIST SP 800-53 Rev 4: MA-4 c; NIST SP 800-53 Rev 5: MA-4 c) |
| Description: | Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> "Allow Basic authentication" to "Disabled". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1126<br>Result: false<br>Title: WN16-CC-000530<br>Description: The Windows Remote Management (WinRM) service must not use Basic authentication.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Allow Basic authentication' is set to 'Disabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112600 (registry_test)<br>Result: false<br>Title: 'Allow Basic authentication' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Service'<br>◦ name must be equal to 'AllowBasic'<br>State ID: oval:mil.disa.stig.windows:ste:112600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-225046 - Anonymous enumeration of shares must not be allowed.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225046r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000270 |
| Identities: | CCE-46305-9<br>SV-88333<br>V-73669<br>CCI-001090 (NIST SP 800-53: SC-4; NIST SP 800-53A: SC-4.1; NIST SP 800-53 Rev 4: SC-4; NIST SP 800-53 Rev 5: SC-4) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1206<br>Result: false<br>Title: Restrict Anonymous Network Shares<br>Description: Anonymous enumeration of shares must be restricted.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:120600 (registry_test)<br>Result: false<br>Title: 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:120600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Control\Lsa'<br>◦ name must be equal to 'RestrictAnonymous'<br>State ID: oval:mil.disa.stig.windows:ste:120600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: [ false ] ◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'System\CurrentControlSet\Control\Lsa'<br>◦ name equals 'RestrictAnonymous'<br>◦ last_write_time equals '133302938190000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

## V-225054 - The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225054r857283_rule |
| Result: | Fail |
| Version: | WN16-SO-000380 |
| Identities: | CCE-46565-8<br>SV-88355<br>V-73691<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |

| | |
|---|---|
| Description: | 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 or nondomain-joined computers that are running later versions. false |
| Fix Text: | 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". |
| Severity: | high |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1217<br>Result: false<br>Title: LanMan Authentication Level<br>Description: The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121700 (registry_test)<br>Result: false<br>Title: 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa'<br>◦ name must be equal to 'LmCompatibilityLevel'<br>State ID: oval:mil.disa.stig.windows:ste:121700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '5'<br>Additional Information: Check existence requirement not met. |

# Detailed Results: Medium Severity (CAT II)

### V-224856 - The Server Message Block (SMB) v1 protocol must be uninstalled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224856r569186_rule |
| Result: | Fail |
| Version: | WN16-00-000410 |
| Identities: | V-73299<br>SV-87951<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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. false |
| Fix Text: | Uninstall the SMBv1 protocol.<br><br>Open "Windows PowerShell" with elevated privileges (run as administrator).<br><br>Enter "Uninstall-WindowsFeature -Name FS-SMB1 -Restart".<br>(Omit the Restart parameter if an immediate restart of the system cannot be done.)<br><br>Alternately:<br><br>Start "Server Manager".<br><br>Select the server with the feature.<br><br>Scroll down to "ROLES AND FEATURES" in the right pane.<br><br>Select "Remove Roles and Features" from the drop-down "TASKS" list.<br><br>Select the appropriate server on the "Server Selection" page and click "Next".<br><br>Deselect "SMB 1.0/CIFS File Sharing Support" on the "Features" page.<br><br>Click "Next" and "Remove" as prompted. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

| | |
|---|---|
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1259<br>Result: false<br>Title: WN16-00-000410<br>Description: The Server Message Block (SMB) v1 protocol must be uninstalled.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Configure SMBv1 Server' is set to 'Disabled')<br>▪ false (All child checks must be true.)<br>▪ false ('Configure SMBv1 client driver' is set to 'Enabled' with 'Disable driver (recommended)' selected for 'Configure MrxSmb10 driver')<br>▪ false (All child checks must be true.)<br>▪ false ('SMB 1.0/CIFS File Sharing Support' feature is not installed) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:16900 (registry_test)<br>Result: false<br>Title: 'Configure SMBv1 Server' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:16900 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters'<br>◦ name must be equal to 'SMB1'<br>State ID: oval:mil.disa.stig.windows:ste:16900 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.windows:tst:17000 (registry_test)<br>Result: false<br>Title: 'Configure SMBv1 client driver' is set to 'Enabled' with 'Disable driver (recommended)' selected for 'Configure MrxSmb10 driver'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:17000 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\mrxsmb10'<br>◦ name must be equal to 'Start'<br>State ID: oval:mil.disa.stig.windows:ste:17000 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '4'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'SYSTEM\CurrentControlSet\Services\mrxsmb10'<br>◦ name equals 'Start'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '2'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.stig.windows:tst:16800 (wmi57_test)<br>Result: false<br>Title: 'SMB 1.0/CIFS File Sharing Support' feature is not installed<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:16800 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>State ID: oval:mil.disa.stig.windows:ste:16800 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ at least one installstate must be equal to '2'<br>Collected Item/State Result: [ false ]<br>◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>◦ collected 'result' result:<br>▪ installstate = '1'<br>Additional Information: Check requirement not met.<br>result |

## V-224857 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224857r569186_rule |
| Result: | Fail |
| Version: | WN16-00-000411 |
| Identities: | V-78123<br>SV-92829<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> "Configure SMBv1 Server" to "Disabled".<br><br>The system must be restarted for the change to take effect.<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1260<br>Result: false<br>Title: WN16-00-000411<br>Description: The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Configure SMBv1 Server' is set to 'Disabled')<br>▪ false (All child checks must be true.)<br>▪ false ('SMB 1.0/CIFS File Sharing Support' feature is not installed) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:16900 (registry_test)<br>Result: false<br>Title: 'Configure SMBv1 Server' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:16900 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters'<br>◦ name must be equal to 'SMB1'<br>State ID: oval:mil.disa.stig.windows:ste:16900 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.windows:tst:16800 (wmi57_test)<br>Result: false<br>Title: 'SMB 1.0/CIFS File Sharing Support' feature is not installed<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:16800 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>State ID: oval:mil.disa.stig.windows:ste:16800 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ at least one installstate must be equal to '2'<br>Collected Item/State Result: [ false ]<br>◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>◦ collected 'result' result:<br>▪ installstate = '1'<br>Additional Information: Check requirement not met.<br>result |

## V-224858 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224858r569186_rule |
| Result: | Fail |
| Version: | WN16-00-000412 |
| Identities: | V-78125<br>SV-92831<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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. false |
| Fix Text: | 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".<br><br>The system must be restarted for the changes to take effect.<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

| | |
|---|---|
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1261<br>Result: false<br>Title: WN16-00-000412<br>Description: The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Configure SMBv1 client driver' is set to 'Enabled' with 'Disable driver (recommended)' selected for 'Configure MrxSmb10 driver')<br>▪ false (All child checks must be true.)<br>▪ false ('SMB 1.0/CIFS File Sharing Support' feature is not installed) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:17000 (registry_test)<br>Result: false<br>Title: 'Configure SMBv1 client driver' is set to 'Enabled' with 'Disable driver (recommended)' selected for 'Configure MrxSmb10 driver'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:17000 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\mrxsmb10'<br>◦ name must be equal to 'Start'<br>State ID: oval:mil.disa.stig.windows:ste:17000 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '4'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'SYSTEM\CurrentControlSet\Services\mrxsmb10'<br>◦ name equals 'Start'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '2'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.stig.windows:tst:16800 (wmi57_test)<br>Result: false<br>Title: 'SMB 1.0/CIFS File Sharing Support' feature is not installed<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:16800 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>State ID: oval:mil.disa.stig.windows:ste:16800 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ at least one installstate must be equal to '2'<br>Collected Item/State Result: [ false ]<br>◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT installstate FROM win32_optionalfeature WHERE name = 'SMB1Protocol''<br>◦ collected 'result' result:<br>▪ installstate = '1'<br>Additional Information: Check requirement not met.<br>result |

## V-224866 - Windows 2016 account lockout duration must be configured to 15 minutes or greater.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224866r852301_rule |
| Result: | Fail |
| Version: | WN16-AC-000010 |
| Identities: | CCE-47152-4<br>SV-87961<br>V-73309<br>CCI-002238 (NIST SP 800-53 Rev 4: AC-7 b; NIST SP 800-53 Rev 5: AC-7 b) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout duration" to "15" minutes or greater.<br><br>A value of "0" is also acceptable, requiring an administrator to unlock the account. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1011<br>Result: false<br>Title: Lockout Duration<br>Description: Lockout duration must meet minimum requirements.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ true ('Account lockout duration' is set to '0')<br>▪ false ('Account lockout threshold' is not set to '0') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:101100 (lockoutpolicy_test)<br>Result: true<br>Title: 'Account lockout duration' is set to '0'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: One or more item-state comparisons may be true.<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101100 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_duration must be less than or equal to '0'<br>State ID: oval:mil.disa.stig.windows:ste:101101 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_duration must be equal to '4294967295'<br>State ID: oval:mil.disa.stig.windows:ste:101102 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_duration must be greater than or equal to '900'<br><br>Test ID: oval:mil.disa.stig.windows:tst:101201 (lockoutpolicy_test)<br>Result: false<br>Title: 'Account lockout threshold' is not set to '0'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101201 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_threshold must be greater than '0'<br>Collected Item/State Result: [ false ] ◦ force_logoff equals '4294967295' ◦ lockout_duration equals '1800' ◦ lockout_observation_window equals '1800' ◦ lockout_threshold equals '0'<br>Additional Information: Check requirement not met.<br>lockout_threshold |

## V-224867 - Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224867r569186_rule |
| Result: | Fail |
| Version: | WN16-AC-000020 |
| Identities: | CCE-46497-4<br>SV-87963<br>V-73311<br>CCI-000044 (NIST SP 800-53: AC-7 a; NIST SP 800-53A: AC-7.1 (ii); NIST SP 800-53 Rev 4: AC-7 a; NIST SP 800-53 Rev 5: AC-7 a) |
| Description: | 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. false |
| Fix Text: | 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). |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1012<br>Result: false<br>Title: Bad Logon Attempts<br>Description: The number of allowed bad logon attempts must meet minimum requirements.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.) ▪ true ('Account lockout threshold' is set to '3' or less) ▪ false ('Account lockout threshold' is not set to '0') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:101200 (lockoutpolicy_test)<br>Result: true<br>Title: 'Account lockout threshold' is set to '3' or less<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101200 (lockoutpolicy_state)<br>State Requirements: ◦ for check = 'all', lockout_threshold, the following must be true:<br>▪ lockout_threshold must be less than or equal to '3'<br><br>Test ID: oval:mil.disa.stig.windows:tst:101201 (lockoutpolicy_test)<br>Result: false<br>Title: 'Account lockout threshold' is not set to '0'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101201 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_threshold must be greater than '0'<br>Collected Item/State Result: [ false ] ◦ force_logoff equals '4294967295'<br>◦ lockout_duration equals '1800'<br>◦ lockout_observation_window equals '1800'<br>◦ lockout_threshold equals '0'<br>Additional Information: Check requirement not met.<br>lockout_threshold |

## V-224868 - Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224868r852302_rule |
| Result: | Fail |
| Version: | WN16-AC-000030 |
| Identities: | CCE-47272-0<br>SV-87965<br>V-73313<br>CCI-000044 (NIST SP 800-53: AC-7 a; NIST SP 800-53A: AC-7.1 (ii); NIST SP 800-53 Rev 4: AC-7 a; NIST SP 800-53 Rev 5: AC-7 a)<br>CCI-002238 (NIST SP 800-53 Rev 4: AC-7 b; NIST SP 800-53 Rev 5: AC-7 b) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128 false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1013<br>Result: false<br>Title: Bad Logon Counter Reset<br>Description: The time before the bad-logon counter is reset must meet minimum requirements.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ true ('Reset account lockout counter after' is set to at least '15' minutes)<br>▪ false ('Account lockout threshold' is not set to '0') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:101300 (lockoutpolicy_test)<br>Result: true<br>Title: 'Reset account lockout counter after' is set to at least '15' minutes<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101300 (lockoutpolicy_state)<br>State Requirements: ◦ for check = 'all', lockout_observation_window, the following must be true:<br>▪ lockout_observation_window must be greater than or equal to '900'<br><br>Test ID: oval:mil.disa.stig.windows:tst:101201 (lockoutpolicy_test)<br>Result: false<br>Title: 'Account lockout threshold' is not set to '0'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101200 (lockoutpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101201 (lockoutpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', lockout_threshold must be greater than '0'<br>Collected Item/State Result: ◦ force_logoff equals '4294967295'<br>[ false ] ◦ lockout_duration equals '1800'<br>◦ lockout_observation_window equals '1800'<br>◦ lockout_threshold equals '0'<br>Additional Information: Check requirement not met.<br>lockout_threshold |

## V-224869 - Windows Server 2016 password history must be configured to 24 passwords remembered.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224869r569186_rule |
| Result: | Fail |
| Version: | WN16-AC-000040 |
| Identities: | CCE-44479-4<br>V-73315<br>SV-87967<br>CCI-000200 (NIST SP 800-53: IA-5 (1) (e); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (e)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Enforce password history" to "24" passwords remembered. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1014<br>Result: false<br>Title: Password Uniqueness<br>Description: Password uniqueness must meet minimum requirements.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Enforce password history' is set to '24' passwords or more) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:101400 (passwordpolicy_test)<br>Result: false<br>Title: 'Enforce password history' is set to '24' passwords or more<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101500 (passwordpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101400 (passwordpolicy_state)<br>State Requirements: ◦ for check = 'all', password_hist_len, the following must be true:<br>▪ password_hist_len must be greater than or equal to '24'<br>Collected Item/State Result: ◦ max_passwd_age equals '3628800'<br>[ false ] ◦ min_passwd_age equals '0'<br>◦ min_passwd_len equals '0'<br>◦ password_hist_len equals '0'<br>◦ password_complexity equals '1'<br>◦ reversible_encryption equals '0'<br>◦ anonymous_name_lookup equals '0'<br>Additional Information: Check requirement not met.<br>password_hist_len |

## V-224871 - Windows Server 2016 minimum password age must be configured to at least one day.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224871r569186_rule |

| | |
|---|---|
| Result: | Fail |
| Version: | WN16-AC-000060 |
| Identities: | CCE-45608-7<br>V-73319<br>SV-87971<br>CCI-000198 (NIST SP 800-53: IA-5 (1) (d); NIST SP 800-53A: IA-5 (1).1 (v); NIST SP 800-53 Rev 4: IA-5 (1) (d)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Minimum password age" to at least "1" day. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1016<br>Result: false<br>Title: Minimum Password Age<br>Description: The minimum password age must meet requirements.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Minimum Password Age' is set to at least '1' day) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:101600 (passwordpolicy_test)<br>Result: false<br>Title: 'Minimum Password Age' is set to at least '1' day<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101500 (passwordpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.windows:ste:101600 (passwordpolicy_state)<br>State Requirements: ◦ for check = 'all', min_passwd_age, the following must be true:<br>▪ min_passwd_age must be greater than or equal to '86400'<br>Collected Item/State Result: ◦ max_passwd_age equals '3628800'<br>[ false ] ◦ min_passwd_age equals '0'<br>◦ min_passwd_len equals '0'<br>◦ password_hist_len equals '0'<br>◦ password_complexity equals '1'<br>◦ reversible_encryption equals '0'<br>◦ anonymous_name_lookup equals '0'<br>Additional Information: Check requirement not met.<br>min_passwd_age |

## V-224872 - Windows Server 2016 minimum password length must be configured to 14 characters.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224872r569186_rule |
| Result: | Fail |
| Version: | WN16-AC-000070 |
| Identities: | V-73321<br>SV-87973<br>CCI-000205 (NIST SP 800-53: IA-5 (1) (a); NIST SP 800-53A: IA-5 (1).1 (i); NIST SP 800-53 Rev 4: IA-5 (1) (a)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Minimum password length" to "14" characters. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:224872<br>Result: false<br>Title: WN16-AC-000070 - Windows Server 2016 minimum password length must be configured to 14 characters.<br>Description: 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.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Minimum password length' is set to at least '14' characters) |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.win:tst:25330300 (passwordpolicy_test)<br>Result: false<br>Title: 'Minimum password length' is set to at least '14' characters<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.win:obj:20000002 (passwordpolicy_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.stig.win:ste:25330300 (passwordpolicy_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', min_passwd_len must be greater than or equal to '14'<br>Collected Item/State Result: [ false ] ◦ max_passwd_age equals '3628800'<br>◦ min_passwd_age equals '0'<br>◦ min_passwd_len equals '0'<br>◦ password_hist_len equals '0'<br>◦ password_complexity equals '1'<br>◦ reversible_encryption equals '0'<br>◦ anonymous_name_lookup equals '0'<br>Additional Information: Check requirement not met.<br>min_passwd_len |

## V-224882 - Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224882r569186_rule |
| Result: | Fail |
| Version: | WN16-AU-000080 |
| Identities: | CCE-44732-6<br>SV-88067<br>V-73415<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c) |
| Description: | 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.<br><br>Credential Validation records events related to validation tests on credentials for a user account logon. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1056<br>Result: false<br>Title: Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.<br>Description: The system must be configured to audit Account Logon - Credential Validation failures.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - Credential Validation - Failure only)<br>▪ false (Audit - Credential Validation - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:466500 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Credential Validation - Failure only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:466500 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', credential_validation must be equal to 'AUDIT_FAILURE' |

| | |
|---|---|
| Collected Item/State Result: [ false ] | • credential_validation equals 'AUDIT_SUCCESS'<br>• kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>• kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>• kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>• other_account_logon_events equals 'AUDIT_NONE'<br>• application_group_management equals 'AUDIT_NONE'<br>• computer_account_management equals 'AUDIT_SUCCESS'<br>• distribution_group_management equals 'AUDIT_NONE'<br>• other_account_management_events equals 'AUDIT_NONE'<br>• security_group_management equals 'AUDIT_SUCCESS'<br>• user_account_management equals 'AUDIT_SUCCESS'<br>• dpapi_activity equals 'AUDIT_NONE'<br>• process_creation equals 'AUDIT_NONE'<br>• process_termination equals 'AUDIT_NONE'<br>• rpc_events equals 'AUDIT_NONE'<br>• directory_service_access equals 'AUDIT_SUCCESS'<br>• directory_service_changes equals 'AUDIT_NONE'<br>• directory_service_replication equals 'AUDIT_NONE'<br>• detailed_directory_service_replication equals 'AUDIT_NONE'<br>• account_lockout equals 'AUDIT_SUCCESS'<br>• ipsec_extended_mode equals 'AUDIT_NONE'<br>• ipsec_main_mode equals 'AUDIT_NONE'<br>• ipsec_quick_mode equals 'AUDIT_NONE'<br>• logoff equals 'AUDIT_SUCCESS'<br>• logon equals 'AUDIT_SUCCESS_FAILURE'<br>• network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>• other_logon_logoff_events equals 'AUDIT_NONE'<br>• special_logon equals 'AUDIT_SUCCESS'<br>• logon_claims equals 'AUDIT_NONE'<br>• application_generated equals 'AUDIT_NONE'<br>• certification_services equals 'AUDIT_NONE'<br>• detailed_file_share equals 'AUDIT_NONE'<br>• file_share equals 'AUDIT_NONE'<br>• file_system equals 'AUDIT_NONE'<br>• filtering_platform_connection equals 'AUDIT_NONE'<br>• filtering_platform_packet_drop equals 'AUDIT_NONE'<br>• handle_manipulation equals 'AUDIT_NONE'<br>• kernel_object equals 'AUDIT_NONE'<br>• other_object_access_events equals 'AUDIT_NONE'<br>• registry equals 'AUDIT_NONE'<br>• sam equals 'AUDIT_NONE'<br>• removable_storage equals 'AUDIT_NONE'<br>• central_access_policy_staging equals 'AUDIT_NONE'<br>• audit_policy_change equals 'AUDIT_SUCCESS'<br>• authentication_policy_change equals 'AUDIT_SUCCESS'<br>• authorization_policy_change equals 'AUDIT_NONE'<br>• filtering_platform_policy_change equals 'AUDIT_NONE'<br>• mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>• other_policy_change_events equals 'AUDIT_NONE'<br>• non_sensitive_privilege_use equals 'AUDIT_NONE'<br>• other_privilege_use_events equals 'AUDIT_NONE'<br>• sensitive_privilege_use equals 'AUDIT_NONE'<br>• ipsec_driver equals 'AUDIT_NONE'<br>• other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>• security_state_change equals 'AUDIT_SUCCESS'<br>• security_system_extension equals 'AUDIT_NONE'<br>• system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>• group_membership equals 'AUDIT_NONE'<br>• pnp_activity equals 'AUDIT_NONE'<br>• user_device_claims equals 'AUDIT_NONE'<br>• audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>credential_validation |

| | |
|---|---|
| Test ID: | oval:mil.disa.fso.windows:tst:466401 (auditeventpolicysubcategories_test) |
| Result: | false |
| Title: | Audit - Credential Validation - Success and Failure |
| Check Existence: | One or more collected items must exist. |
| Check: | All collected items must match the given state(s). |
| Object ID: | oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |
| Object Requirements: | • Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:466401 (auditeventpolicysubcategories_state) |
| State Requirements: | • check_existence = 'at_least_one_exists', credential_validation must be equal to 'AUDIT_SUCCESS_FAILURE' |

| | |
|---|---|
| Collected Item/State Result: [ false ] | • credential_validation equals 'AUDIT_SUCCESS'<br>• kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>• kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>• kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>• other_account_logon_events equals 'AUDIT_NONE'<br>• application_group_management equals 'AUDIT_NONE'<br>• computer_account_management equals 'AUDIT_SUCCESS'<br>• distribution_group_management equals 'AUDIT_NONE'<br>• other_account_management_events equals 'AUDIT_NONE'<br>• security_group_management equals 'AUDIT_SUCCESS'<br>• user_account_management equals 'AUDIT_SUCCESS'<br>• dpapi_activity equals 'AUDIT_NONE'<br>• process_creation equals 'AUDIT_NONE'<br>• process_termination equals 'AUDIT_NONE'<br>• rpc_events equals 'AUDIT_NONE'<br>• directory_service_access equals 'AUDIT_SUCCESS'<br>• directory_service_changes equals 'AUDIT_NONE'<br>• directory_service_replication equals 'AUDIT_NONE'<br>• detailed_directory_service_replication equals 'AUDIT_NONE'<br>• account_lockout equals 'AUDIT_SUCCESS'<br>• ipsec_extended_mode equals 'AUDIT_NONE'<br>• ipsec_main_mode equals 'AUDIT_NONE'<br>• ipsec_quick_mode equals 'AUDIT_NONE'<br>• logoff equals 'AUDIT_SUCCESS'<br>• logon equals 'AUDIT_SUCCESS_FAILURE'<br>• network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>• other_logon_logoff_events equals 'AUDIT_NONE'<br>• special_logon equals 'AUDIT_SUCCESS'<br>• logon_claims equals 'AUDIT_NONE'<br>• application_generated equals 'AUDIT_NONE'<br>• certification_services equals 'AUDIT_NONE'<br>• detailed_file_share equals 'AUDIT_NONE'<br>• file_share equals 'AUDIT_NONE'<br>• file_system equals 'AUDIT_NONE'<br>• filtering_platform_connection equals 'AUDIT_NONE'<br>• filtering_platform_packet_drop equals 'AUDIT_NONE'<br>• handle_manipulation equals 'AUDIT_NONE'<br>• kernel_object equals 'AUDIT_NONE'<br>• other_object_access_events equals 'AUDIT_NONE'<br>• registry equals 'AUDIT_NONE'<br>• sam equals 'AUDIT_NONE'<br>• removable_storage equals 'AUDIT_NONE'<br>• central_access_policy_staging equals 'AUDIT_NONE'<br>• audit_policy_change equals 'AUDIT_SUCCESS'<br>• authentication_policy_change equals 'AUDIT_SUCCESS'<br>• authorization_policy_change equals 'AUDIT_NONE'<br>• filtering_platform_policy_change equals 'AUDIT_NONE'<br>• mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>• other_policy_change_events equals 'AUDIT_NONE'<br>• non_sensitive_privilege_use equals 'AUDIT_NONE'<br>• other_privilege_use_events equals 'AUDIT_NONE'<br>• sensitive_privilege_use equals 'AUDIT_NONE'<br>• ipsec_driver equals 'AUDIT_NONE'<br>• other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>• security_state_change equals 'AUDIT_SUCCESS'<br>• security_system_extension equals 'AUDIT_NONE'<br>• system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>• group_membership equals 'AUDIT_NONE'<br>• pnp_activity equals 'AUDIT_NONE'<br>• user_device_claims equals 'AUDIT_NONE'<br>• audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>credential_validation |

## V-224883 - Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224883r652305_rule |
| Result: | Fail |
| Version: | WN16-AU-000100 |
| Identities: | CCE-45973-5<br>SV-88071<br>V-73419<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Other Account Management Events records events such as the access of a password hash or the Password Policy Checking API being called.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210<br>false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1057
Result: false
Title: Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.
Description: The system must be configured to audit Account Management - Other Account Management Events successes.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false (Audit - Other Account Management Events - Success only)
    - false (Audit - Other Account Management Events - Success and Failure)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:466800 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Other Account Management Events - Success only
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:466800 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', other_account_management_events must be equal to 'AUDIT_SUCCESS'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
other_account_management_events

---

Test ID: oval:mil.disa.fso.windows:tst:466801 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Other Account Management Events - Success and Failure
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:466801 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', other_account_management_events must be equal to 'AUDIT_SUCCESS_FAILURE'

| | |
|---|---|
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>other_account_management_events |

## V-224886 - Windows Server 2016 must be configured to audit Account Management - User Account Management failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224886r852308_rule |
| Result: | Fail |
| Version: | WN16-AU-000150 |
| Identities: | CCE-46552-6<br>SV-88081<br>V-73429<br>CCI-000018 (NIST SP 800-53: AC-2 (4); NIST SP 800-53A: AC-2 (4).1 (i and ii); NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4))<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-001403 (NIST SP 800-53: AC-2 (4); NIST SP 800-53A: AC-2 (4).1 (i and ii); NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4))<br>CCI-001404 (NIST SP 800-53: AC-2 (4); NIST SP 800-53A: AC-2 (4).1 (i and ii); NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4))<br>CCI-001405 (NIST SP 800-53: AC-2 (4); NIST SP 800-53A: AC-2 (4).1 (i and ii); NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4))<br>CCI-002130 (NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4)) |
| Description: | 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.<br><br>User Account Management records events such as creating, changing, deleting, renaming, disabling, or enabling user accounts.<br><br>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 false |
| Fix Text: | 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. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1062<br>Result: false<br>Title: Windows Server 2016 must be configured to audit Account Management - User Account Management failures.<br>Description: The system must be configured to audit Account Management - User Account Management failures.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - User Account Management - Failure only)<br>▪ false (Audit - User Account Management - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:467300 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - User Account Management - Failure only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:467300 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', user_account_management must be equal to 'AUDIT_FAILURE'<br>Collected Item/State Result: [ false ]<br>◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'<br>Additional Information: Check requirement not met.<br>user_account_management<br><br>Test ID: oval:mil.disa.fso.windows:tst:467201 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - User Account Management - Success and Failure<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |

| | |
|---|---|
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:467201 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', user_account_management must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>user_account_management |

### V-224888 - Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224888r852309_rule |
| Result: | Fail |
| Version: | WN16-AU-000170 |
| Identities: | CCE-46177-2<br>SV-88085<br>V-73433<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Process Creation records events related to the creation of a process and the source.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000471-GPOS-00215 false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1063
Result: false

Title: Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.
Description: The system must be configured to audit Detailed Tracking - Process Creation successes.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false (Audit - Process Creation - Success only)
    - false (Audit - Process Creation - Success and Failure)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:467400 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Process Creation - Success only
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:467400 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', process_creation must be equal to 'AUDIT_SUCCESS'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
process_creation

---

Test ID: oval:mil.disa.fso.windows:tst:467401 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Process Creation - Success and Failure
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:467401 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', process_creation must be equal to 'AUDIT_SUCCESS_FAILURE'

| | |
|---|---|
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>process_creation |

## V-224890 - Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224890r569186_rule |
| Result: | Fail |
| Version: | WN16-AU-000230 |
| Identities: | SV-88097<br>V-73445<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-001404 (NIST SP 800-53: AC-2 (4); NIST SP 800-53A: AC-2 (4).1 (i and ii); NIST SP 800-53 Rev 4: AC-2 (4); NIST SP 800-53 Rev 5: AC-2 (4)) |
| Description: | 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.<br><br>Account Lockout events can be used to identify potentially malicious logon attempts.<br><br>Satisfies: SRG-OS-000240-GPOS-00090, SRG-OS-000470-GPOS-00214 false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1268
Result: false
Title: WN16-AU-000230
Description: Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false ('Audit Account Lockout' is set to 'Failure')
    - false ('Audit Account Lockout' is set to 'Success' and 'Failure')

Tests:

Test ID: oval:mil.disa.stig.windows:tst:14700 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Account Lockout' is set to 'Failure'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:394100 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:14700 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', account_lockout must be equal to 'AUDIT_FAILURE'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
account_lockout

---

Test ID: oval:mil.disa.stig.windows:tst:11901 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Account Lockout' is set to 'Success' and 'Failure'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).

Object ID: oval:mil.disa.fso.windows:obj:394100 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

| | |
|---|---|
| State ID: | oval:mil.disa.stig.windows:ste:11901 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', account_lockout must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>account_lockout |

## V-224896 - Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224896r569186_rule |
| Result: | Fail |
| Version: | WN16-AU-000285 |
| Identities: | CCE-45980-0<br>SV-101009<br>V-90359<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c) |
| Description: | 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.<br><br>Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> "Audit Other Object Access Events" with "Success" selected. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1274
Result: false
Title: WN16-AU-000285
Description: Windows Server 2016 must be configured to audit Object Access - Other Object Access Events successes.
Class: compliance
Tests:
- false (One or more child checks must be true.)
  - false ('Audit Other Object Access Events' is set to 'Success')
  - false ('Audit Other Object Access Events' is set to 'Success' and 'Failure')

Tests:

Test ID: oval:mil.disa.stig.windows:tst:127400 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Other Object Access Events' is set to 'Success'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:105500 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:127400 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', other_object_access_events must be equal to 'AUDIT_SUCCESS'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
other_object_access_events

---

Test ID: oval:mil.disa.stig.windows:tst:127501 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Other Object Access Events' is set to 'Success' and 'Failure'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:105500 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:127501 (auditeventpolicysubcategories_state)

| | |
|---|---|
| State Requirements: | ◦ check_existence = 'at_least_one_exists', other_object_access_events must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>other_object_access_events |

## V-224897 - Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224897r569186_rule |
| Result: | Fail |
| Version: | WN16-AU-000286 |
| Identities: | CCE-45980-0<br>SV-101011<br>V-90361<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c) |
| Description: | 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.<br><br>Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> "Audit Other Object Access Events" with "Failure" selected. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1275
Result: false
Title: WN16-AU-000286
Description: Windows Server 2016 must be configured to audit Object Access - Other Object Access Events failures.
Class: compliance
Tests:
- false (One or more child checks must be true.)
  - false ('Audit Other Object Access Events' is set to 'Failure')
  - false ('Audit Other Object Access Events' is set to 'Success' and 'Failure')

Tests:

Test ID: oval:mil.disa.stig.windows:tst:127500 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Other Object Access Events' is set to 'Failure'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:105500 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:127500 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', other_object_access_events must be equal to 'AUDIT_FAILURE'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
other_object_access_events

---

Test ID: oval:mil.disa.stig.windows:tst:127501 (auditeventpolicysubcategories_test)
Result: false
Title: 'Audit Other Object Access Events' is set to 'Success' and 'Failure'
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:105500 (auditeventpolicysubcategories_object)

Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:127501 (auditeventpolicysubcategories_state)

| | |
|---|---|
| State Requirements: | ◦ check_existence = 'at_least_one_exists', other_object_access_events must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>other_object_access_events |

### V-224901 - Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224901r852311_rule |
| Result: | Fail |
| Version: | WN16-AU-000320 |
| Identities: | CCE-45966-9<br>SV-88115<br>V-73463<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Audit Policy Change records events related to changes in audit policy.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212<br>false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1071
Result: false
Title: Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.
Description: The system must be configured to audit Policy Change - Audit Policy Change failures.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false (Audit - Audit Policy Change - Failure only)
    - false (Audit - Audit Policy Change - Success and Failure)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:468200 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Audit Policy Change - Failure only
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:468200 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', audit_policy_change must be equal to 'AUDIT_FAILURE'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
audit_policy_change

---

Test ID: oval:mil.disa.fso.windows:tst:468101 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Audit Policy Change - Success and Failure
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

| | |
|---|---|
| State ID: | oval:mil.disa.fso.windows:ste:468101 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', audit_policy_change must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>audit_policy_change |

## V-224903 - Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224903r852313_rule |
| Result: | Fail |
| Version: | WN16-AU-000340 |
| Identities: | CCE-46306-7<br>SV-88119<br>V-73467<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Authorization Policy Change records events related to changes in user rights, such as "Create a token object".<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210<br>false |
| Fix Text: | 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. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1073<br>Result: false<br>Title: Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.<br>Description: The system must be configured to audit Policy Change - Audit Policy Change successes.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - Audit Policy Change - Success only)<br>▪ false (Audit - Audit Policy Change - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:497500 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Audit Policy Change - Success only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:497500 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', authorization_policy_change must be equal to 'AUDIT_SUCCESS'<br>Collected Item/State Result: [ false ]<br>◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'<br>Additional Information: Check requirement not met.<br>authorization_policy_change<br><br>Test ID: oval:mil.disa.fso.windows:tst:497501 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Audit Policy Change - Success and Failure<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |

| | |
|---|---|
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:497501 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', authorization_policy_change must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>authorization_policy_change |

## V-224904 - Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224904r852314_rule |
| Result: | Fail |
| Version: | WN16-AU-000350 |
| Identities: | CCE-45981-8<br>SV-88121<br>V-73469<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Sensitive Privilege Use records events related to use of sensitive privileges, such as "Act as part of the operating system" or "Debug programs".<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210<br>false |
| Fix Text: | 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. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1074<br>Result: false<br>Title: Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.<br>Description: The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - Sensitive Privilege Use - Success only)<br>▪ false (Audit - Sensitive Privilege Use - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:468400 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Sensitive Privilege Use - Success only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:468400 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', sensitive_privilege_use must be equal to 'AUDIT_SUCCESS'<br>Collected Item/State Result: [ false ]<br>◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'<br>Additional Information: Check requirement not met.<br>sensitive_privilege_use<br>---<br>Test ID: oval:mil.disa.fso.windows:tst:468401 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Sensitive Privilege Use - Success and Failure<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |

| | |
|---|---|
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:468401 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', sensitive_privilege_use must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>sensitive_privilege_use |

### V-224905 - Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224905r852315_rule |
| Result: | Fail |
| Version: | WN16-AU-000360 |
| Identities: | CCE-45981-8<br>SV-88123<br>V-73471<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Sensitive Privilege Use records events related to use of sensitive privileges, such as "Act as part of the operating system" or "Debug programs".<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210<br>false |
| Fix Text: | 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. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1075<br>Result: false<br>Title: Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.<br>Description: The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - Sensitive Privilege Use - Failure only)<br>▪ false (Audit - Sensitive Privilege Use - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:468500 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Sensitive Privilege Use - Failure only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:468500 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', sensitive_privilege_use must be equal to 'AUDIT_FAILURE'<br>Collected Item/State Result: [ false ] ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'<br>Additional Information: Check requirement not met.<br>sensitive_privilege_use<br><br>Test ID: oval:mil.disa.fso.windows:tst:468401 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - Sensitive Privilege Use - Success and Failure<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |

| | |
|---|---|
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:468401 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', sensitive_privilege_use must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>sensitive_privilege_use |

## V-224906 - Windows Server 2016 must be configured to audit System - IPsec Driver successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224906r852316_rule |
| Result: | Fail |
| Version: | WN16-AU-000370 |
| Identities: | CCE-46482-6<br>SV-88125<br>V-73473<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>IPsec Driver records events related to the IPsec Driver, such as dropped packets.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212<br>false |
| Fix Text: | 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. |
| Severity: | medium |

| | |
|---|---|
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1076<br>Result: false<br>Title: Windows Server 2016 must be configured to audit System - IPsec Driver successes.<br>Description: The system must be configured to audit System - IPsec Driver successes.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (One or more child checks must be true.)<br>▪ false (Audit - IPSec Driver - Success only)<br>▪ false (Audit - IPSec Driver - Success and Failure) |
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:468600 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - IPSec Driver - Success only<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)<br>Object Requirements: ◦ Collect any available items.<br>State ID: oval:mil.disa.fso.windows:ste:468600 (auditeventpolicysubcategories_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', ipsec_driver must be equal to 'AUDIT_SUCCESS'<br>Collected Item/State Result: [ false ]<br>◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'<br>Additional Information: Check requirement not met.<br>ipsec_driver<br><br>Test ID: oval:mil.disa.fso.windows:tst:468601 (auditeventpolicysubcategories_test)<br>Result: false<br>Title: Audit - IPSec Driver - Success and Failure<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object) |

| | |
|---|---|
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.fso.windows:ste:468601 (auditeventpolicysubcategories_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', ipsec_driver must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>ipsec_driver |

## V-224907 - Windows Server 2016 must be configured to audit System - IPsec Driver failures.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224907r852317_rule |
| Result: | Fail |
| Version: | WN16-AU-000380 |
| Identities: | CCE-46482-6<br>SV-88127<br>V-73475<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>IPsec Driver records events related to the IPsec Driver, such as dropped packets.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212<br>false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1077
Result: false
Title: Windows Server 2016 must be configured to audit System - IPsec Driver failures.
Description: The system must be configured to audit System - IPsec Driver failures.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false (Audit - IPSec Driver - Failure only)
    - false (Audit - IPSec Driver - Success and Failure)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:468700 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - IPSec Driver - Failure only
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:468700 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', ipsec_driver must be equal to 'AUDIT_FAILURE'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
ipsec_driver

---

Test ID: oval:mil.disa.fso.windows:tst:468601 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - IPSec Driver - Success and Failure
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:468601 (auditeventpolicysubcategories_state)

| | |
|---|---|
| State Requirements: | ◦ check_existence = 'at_least_one_exists', ipsec_driver must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>ipsec_driver |

## V-224911 - Windows Server 2016 must be configured to audit System - Security System Extension successes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224911r852321_rule |
| Result: | Fail |
| Version: | WN16-AU-000420 |
| Identities: | CCE-47111-0<br>SV-88135<br>V-73483<br>CCI-000172 (NIST SP 800-53: AU-12 c; NIST SP 800-53A: AU-12.1 (iv); NIST SP 800-53 Rev 4: AU-12 c; NIST SP 800-53 Rev 5: AU-12 c)<br>CCI-002234 (NIST SP 800-53 Rev 4: AC-6 (9); NIST SP 800-53 Rev 5: AC-6 (9)) |
| Description: | 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.<br><br>Security System Extension records events related to extension code being loaded by the security subsystem.<br><br>Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000468-GPOS-00212<br>false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |

Reference:

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

Definitions:

Definition ID: oval:mil.disa.stig.windows:def:1079
Result: false
Title: Windows Server 2016 must be configured to audit System - Security System Extension successes.
Description: The system must be configured to audit System - Security System Extension successes.
Class: compliance
Tests:
- false (All child checks must be true.)
  - false (One or more child checks must be true.)
    - false (Audit - Security System Extension - Success only)
    - false (Audit - Security System Extension - Success and Failure)

Tests:

Test ID: oval:mil.disa.fso.windows:tst:469000 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Security System Extension - Success only
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:469000 (auditeventpolicysubcategories_state)
State Requirements:
- check_existence = 'at_least_one_exists', security_system_extension must be equal to 'AUDIT_SUCCESS'

Collected Item/State Result: [ false ]
- credential_validation equals 'AUDIT_SUCCESS'
- kerberos_authentication_service equals 'AUDIT_SUCCESS'
- kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'
- kerberos_ticket_events equals 'AUDIT_SUCCESS'
- other_account_logon_events equals 'AUDIT_NONE'
- application_group_management equals 'AUDIT_NONE'
- computer_account_management equals 'AUDIT_SUCCESS'
- distribution_group_management equals 'AUDIT_NONE'
- other_account_management_events equals 'AUDIT_NONE'
- security_group_management equals 'AUDIT_SUCCESS'
- user_account_management equals 'AUDIT_SUCCESS'
- dpapi_activity equals 'AUDIT_NONE'
- process_creation equals 'AUDIT_NONE'
- process_termination equals 'AUDIT_NONE'
- rpc_events equals 'AUDIT_NONE'
- directory_service_access equals 'AUDIT_SUCCESS'
- directory_service_changes equals 'AUDIT_NONE'
- directory_service_replication equals 'AUDIT_NONE'
- detailed_directory_service_replication equals 'AUDIT_NONE'
- account_lockout equals 'AUDIT_SUCCESS'
- ipsec_extended_mode equals 'AUDIT_NONE'
- ipsec_main_mode equals 'AUDIT_NONE'
- ipsec_quick_mode equals 'AUDIT_NONE'
- logoff equals 'AUDIT_SUCCESS'
- logon equals 'AUDIT_SUCCESS_FAILURE'
- network_policy_server equals 'AUDIT_SUCCESS_FAILURE'
- other_logon_logoff_events equals 'AUDIT_NONE'
- special_logon equals 'AUDIT_SUCCESS'
- logon_claims equals 'AUDIT_NONE'
- application_generated equals 'AUDIT_NONE'
- certification_services equals 'AUDIT_NONE'
- detailed_file_share equals 'AUDIT_NONE'
- file_share equals 'AUDIT_NONE'
- file_system equals 'AUDIT_NONE'
- filtering_platform_connection equals 'AUDIT_NONE'
- filtering_platform_packet_drop equals 'AUDIT_NONE'
- handle_manipulation equals 'AUDIT_NONE'
- kernel_object equals 'AUDIT_NONE'
- other_object_access_events equals 'AUDIT_NONE'
- registry equals 'AUDIT_NONE'
- sam equals 'AUDIT_NONE'
- removable_storage equals 'AUDIT_NONE'
- central_access_policy_staging equals 'AUDIT_NONE'
- audit_policy_change equals 'AUDIT_SUCCESS'
- authentication_policy_change equals 'AUDIT_SUCCESS'
- authorization_policy_change equals 'AUDIT_NONE'
- filtering_platform_policy_change equals 'AUDIT_NONE'
- mpssvc_rule_level_policy_change equals 'AUDIT_NONE'
- other_policy_change_events equals 'AUDIT_NONE'
- non_sensitive_privilege_use equals 'AUDIT_NONE'
- other_privilege_use_events equals 'AUDIT_NONE'
- sensitive_privilege_use equals 'AUDIT_NONE'
- ipsec_driver equals 'AUDIT_NONE'
- other_system_events equals 'AUDIT_SUCCESS_FAILURE'
- security_state_change equals 'AUDIT_SUCCESS'
- security_system_extension equals 'AUDIT_NONE'
- system_integrity equals 'AUDIT_SUCCESS_FAILURE'
- group_membership equals 'AUDIT_NONE'
- pnp_activity equals 'AUDIT_NONE'
- user_device_claims equals 'AUDIT_NONE'
- audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE'

Additional Information: Check requirement not met.
security_system_extension

---

Test ID: oval:mil.disa.fso.windows:tst:469001 (auditeventpolicysubcategories_test)
Result: false
Title: Audit - Security System Extension - Success and Failure
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.fso.windows:obj:466400 (auditeventpolicysubcategories_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.fso.windows:ste:469001 (auditeventpolicysubcategories_state)

| | |
|---|---|
| State Requirements: | ◦ check_existence = 'at_least_one_exists', security_system_extension must be equal to 'AUDIT_SUCCESS_FAILURE' |
| Collected Item/State Result: [ false ] | ◦ credential_validation equals 'AUDIT_SUCCESS'<br>◦ kerberos_authentication_service equals 'AUDIT_SUCCESS'<br>◦ kerberos_service_ticket_operations equals 'AUDIT_SUCCESS'<br>◦ kerberos_ticket_events equals 'AUDIT_SUCCESS'<br>◦ other_account_logon_events equals 'AUDIT_NONE'<br>◦ application_group_management equals 'AUDIT_NONE'<br>◦ computer_account_management equals 'AUDIT_SUCCESS'<br>◦ distribution_group_management equals 'AUDIT_NONE'<br>◦ other_account_management_events equals 'AUDIT_NONE'<br>◦ security_group_management equals 'AUDIT_SUCCESS'<br>◦ user_account_management equals 'AUDIT_SUCCESS'<br>◦ dpapi_activity equals 'AUDIT_NONE'<br>◦ process_creation equals 'AUDIT_NONE'<br>◦ process_termination equals 'AUDIT_NONE'<br>◦ rpc_events equals 'AUDIT_NONE'<br>◦ directory_service_access equals 'AUDIT_SUCCESS'<br>◦ directory_service_changes equals 'AUDIT_NONE'<br>◦ directory_service_replication equals 'AUDIT_NONE'<br>◦ detailed_directory_service_replication equals 'AUDIT_NONE'<br>◦ account_lockout equals 'AUDIT_SUCCESS'<br>◦ ipsec_extended_mode equals 'AUDIT_NONE'<br>◦ ipsec_main_mode equals 'AUDIT_NONE'<br>◦ ipsec_quick_mode equals 'AUDIT_NONE'<br>◦ logoff equals 'AUDIT_SUCCESS'<br>◦ logon equals 'AUDIT_SUCCESS_FAILURE'<br>◦ network_policy_server equals 'AUDIT_SUCCESS_FAILURE'<br>◦ other_logon_logoff_events equals 'AUDIT_NONE'<br>◦ special_logon equals 'AUDIT_SUCCESS'<br>◦ logon_claims equals 'AUDIT_NONE'<br>◦ application_generated equals 'AUDIT_NONE'<br>◦ certification_services equals 'AUDIT_NONE'<br>◦ detailed_file_share equals 'AUDIT_NONE'<br>◦ file_share equals 'AUDIT_NONE'<br>◦ file_system equals 'AUDIT_NONE'<br>◦ filtering_platform_connection equals 'AUDIT_NONE'<br>◦ filtering_platform_packet_drop equals 'AUDIT_NONE'<br>◦ handle_manipulation equals 'AUDIT_NONE'<br>◦ kernel_object equals 'AUDIT_NONE'<br>◦ other_object_access_events equals 'AUDIT_NONE'<br>◦ registry equals 'AUDIT_NONE'<br>◦ sam equals 'AUDIT_NONE'<br>◦ removable_storage equals 'AUDIT_NONE'<br>◦ central_access_policy_staging equals 'AUDIT_NONE'<br>◦ audit_policy_change equals 'AUDIT_SUCCESS'<br>◦ authentication_policy_change equals 'AUDIT_SUCCESS'<br>◦ authorization_policy_change equals 'AUDIT_NONE'<br>◦ filtering_platform_policy_change equals 'AUDIT_NONE'<br>◦ mpssvc_rule_level_policy_change equals 'AUDIT_NONE'<br>◦ other_policy_change_events equals 'AUDIT_NONE'<br>◦ non_sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ other_privilege_use_events equals 'AUDIT_NONE'<br>◦ sensitive_privilege_use equals 'AUDIT_NONE'<br>◦ ipsec_driver equals 'AUDIT_NONE'<br>◦ other_system_events equals 'AUDIT_SUCCESS_FAILURE'<br>◦ security_state_change equals 'AUDIT_SUCCESS'<br>◦ security_system_extension equals 'AUDIT_NONE'<br>◦ system_integrity equals 'AUDIT_SUCCESS_FAILURE'<br>◦ group_membership equals 'AUDIT_NONE'<br>◦ pnp_activity equals 'AUDIT_NONE'<br>◦ user_device_claims equals 'AUDIT_NONE'<br>◦ audit_detailedtracking_tokenrightadjusted equals 'AUDIT_NONE' |
| Additional Information: | Check requirement not met.<br>security_system_extension |

### V-224914 - The display of slide shows on the lock screen must be disabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224914r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000010 |
| Identities: | SV-88145<br>V-73493<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> "Prevent enabling lock screen slide show" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

| | |
|---|---|
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:69<br>Result: false<br><br>Title: The display of slide shows on the lock screen must be disabled.<br>Description: The display of slide shows on the lock screen must be disabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Verifies 'Prevent enabling lock screen slide show' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:6900 (registry_test)<br>Result: false<br>Title: Verifies 'Prevent enabling lock screen slide show' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:6900 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\Personalization'<br>◦ name must be equal to 'NoLockScreenSlideshow'<br>State ID: oval:mil.disa.stig.windows:ste:6900 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224915 - WDigest Authentication must be disabled on Windows Server 2016.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224915r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000030 |
| Identities: | V-73497<br>SV-88149<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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 Server 2016. This setting ensures this is enforced. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> "WDigest Authentication (disabling may require KB2871997)" to "Disabled".<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:148<br>Result: false<br>Title: WDigest Authentication must be disabled<br>Description: WDigest Authentication must be disabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (WDigest Authentication is disabled) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:14800 (registry_test)<br>Result: false<br>Title: WDigest Authentication is disabled<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:14800 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest'<br>◦ name must be equal to 'UseLogonCredential'<br>State ID: oval:mil.disa.stig.windows:ste:14800 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224920 - Insecure logons to an SMB server must be disabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224920r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000080 |
| Identities: | SV-88159<br>V-73507<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | Insecure guest logons allow unauthenticated access to shared folders. Shared resources on a system must require authentication to establish proper access. false |

| | |
|---|---|
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Lanman Workstation >> "Enable insecure guest logons" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1273<br>Result: false<br>Title: WN16-CC-000080<br>Description: Insecure logons to an SMB server must be disabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Enable insecure guest logons' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:420300 (registry_test)<br>Result: false<br>Title: 'Enable insecure guest logons' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:420300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation'<br>◦ name must be equal to 'AllowInsecureGuestAuth'<br>State ID: oval:mil.disa.stig.windows:ste:420300 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

### V-224922 - Command line data must be included in process creation events.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224922r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000100 |
| Identities: | CCE-45411-6<br>V-73511<br>SV-88163<br>CCI-000135 (NIST SP 800-53: AU-3 (1); NIST SP 800-53A: AU-3 (1).1 (ii); NIST SP 800-53 Rev 4: AU-3 (1); NIST SP 800-53 Rev 5: AU-3 (1)) |
| Description: | 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.<br><br>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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Audit Process Creation >> "Include command line in process creation events" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1258<br>Result: false<br>Title: WN16-CC-000100<br>Description: Command line data must be included in process creation events.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Include command line in process creation events' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:17100 (registry_test)<br>Result: false<br>Title: 'Include command line in process creation events' is set to 'Enabled'<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:17100 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit'<br>◦ name must match the pattern 'ProcessCreationIncludeCmdLine_Enabled'<br>State ID: oval:mil.disa.stig.windows:ste:17100 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224925 - Group Policy objects must be reprocessed even if they have not changed.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224925r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000150 |
| Identities: | CCE-46343-0<br>SV-88177<br>V-73525<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1090<br>Result: false<br>Title: WN16-CC-000150<br>Description: Group Policy objects must be reprocessed even if they have not changed.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Configure registry policy processing' is set to 'Enabled' with the option 'Process even if the Group Policy objects have not changed' selected) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109000 (registry_test)<br>Result: false<br>Title: 'Configure registry policy processing' is set to 'Enabled' with the option 'Process even if the Group Policy objects have not changed' selected<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109000 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}'<br>◦ name must be equal to 'NoGPOListChanges'<br>State ID: oval:mil.disa.stig.windows:ste:109000 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224926 - Downloading print driver packages over HTTP must be prevented.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224926r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000160 |
| Identities: | CCE-47107-8<br>V-73527<br>SV-88179<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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.<br><br>This setting prevents the computer from downloading print driver packages over HTTP. false |
| Fix Text: | 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". |

| | |
|---|---|
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1091<br>Result: false<br>Title: WN16-CC-000160<br>Description: Downloading print driver packages over HTTP must be prevented.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Turn off downloading of print drivers over HTTP' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109100 (registry_test)<br>Result: false<br>Title: 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109100 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows NT\Printers'<br>◦ name must be equal to 'DisableWebPnPDownload'<br>State ID: oval:mil.disa.stig.windows:ste:109100 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224927 - Printing over HTTP must be prevented.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224927r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000170 |
| Identities: | CCE-47297-7<br>SV-88181<br>V-73529<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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.<br><br>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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> "Turn off printing over HTTP" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1092<br>Result: false<br>Title: WN16-CC-000170<br>Description: Printing over HTTP must be prevented.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Turn off printing over HTTP' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109200 (registry_test)<br>Result: false<br>Title: 'Turn off printing over HTTP' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109200 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows NT\Printers'<br>◦ name must be equal to 'DisableHTTPPrinting'<br>State ID: oval:mil.disa.stig.windows:ste:109200 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224928 - The network selection user interface (UI) must not be displayed on the logon screen.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224928r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000180 |
| Identities: | V-73531<br>SV-88185<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | Enabling interaction with the network selection UI allows users to change connections to available networks without signing in to Windows. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> "Do not display network selection UI" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:66<br>Result: false<br>Title: The network selection user interface (UI) must not be displayed on the logon screen.<br>Description: The network selection user interface (UI) must not be displayed on the logon screen.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Verifies 'Do not display network selection UI' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:6600 (registry_test)<br>Result: false<br>Title: Verifies 'Do not display network selection UI' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:6600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\System'<br>◦ name must be equal to 'DontDisplayNetworkSelectionUI'<br>State ID: oval:mil.disa.stig.windows:ste:6600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224929 - Users must be prompted to authenticate when the system wakes from sleep (on battery).

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224929r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000210 |
| Identities: | CCE-47317-3<br>SV-88197<br>V-73537<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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). false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1094<br>Result: false<br>Title: WN16-CC-000210<br>Description: Users must be prompted to authenticate when the system wakes from sleep (on battery).<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Require a password when a computer wakes (on battery)' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109400 (registry_test)<br>Result: false<br>Title: 'Require a password when a computer wakes (on battery)' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109400 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51'<br>◦ name must be equal to 'DCSettingIndex'<br>State ID: oval:mil.disa.stig.windows:ste:109400 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224930 - Users must be prompted to authenticate when the system wakes from sleep (plugged in).

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224930r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000220 |
| Identities: | CCE-46919-7<br>SV-88201<br>V-73539<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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). false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1095<br>Result: false<br>Title: WN16-CC-000220<br>Description: Users must be prompted to authenticate when the system wakes from sleep (plugged in).<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false ('Require a password when a computer wakes (plugged in)' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109500 (registry_test)<br>Result: false<br>Title: 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109500 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51'<br>◦ name must be equal to 'ACSettingIndex'<br>State ID: oval:mil.disa.stig.windows:ste:109500 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224935 - Administrator accounts must not be enumerated during elevation.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224935r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000280 |
| Identities: | CCE-46465-1<br>V-73487<br>SV-88139<br>CCI-001084 (NIST SP 800-53: SC-3; NIST SP 800-53A: SC-3.1 (ii); NIST SP 800-53 Rev 4: SC-3; NIST SP 800-53 Rev 5: SC-3) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Credential User Interface >> "Enumerate administrator accounts on elevation" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1104<br>Result: false<br>Title: WN16-CC-000280<br>Description: Windows Server 2016 must require username and password to elevate a running application.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Enumerate administrator accounts on elevation' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:110400 (registry_test)<br>Result: false<br>Title: 'Enumerate administrator accounts on elevation' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:110400 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI'<br>◦ name must be equal to 'EnumerateAdministrators'<br>State ID: oval:mil.disa.stig.windows:ste:110400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224936 - Windows Telemetry must be configured to Security or Basic.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224936r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000290 |
| Identities: | SV-88215<br>V-73551<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:224936<br>Result: false<br>Title: WN16-CC-000290 - Windows Telemetry must be configured to Security or Basic.<br>Description: 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.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Allow Diagnostic Data' is set to 'Enabled' with 'Diagnostic Data Off (Not recommended)' or 'Send Required Diagnostic Data' selected in 'Options:') |
| Tests: | Test ID: oval:mil.disa.stig.win:tst:25339300 (registry_test)<br>Result: false<br>Title: 'Allow Diagnostic Data' is set to 'Enabled' with 'Diagnostic Data Off (Not recommended)' or 'Send Required Diagnostic Data' selected in 'Options:'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: One or more item-state comparisons may be true.<br>Object ID: oval:mil.disa.stig.win:obj:25339300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\DataCollection'<br>◦ name must be equal to 'AllowTelemetry'<br>State ID: oval:mil.disa.stig.win:ste:20000000 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>State ID: oval:mil.disa.stig.win:ste:20000001 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

### V-224937 - The Application event log size must be configured to 32768 KB or greater.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224937r877391_rule |
| Result: | Fail |
| Version: | WN16-CC-000300 |
| Identities: | CCE-44494-3<br>SV-88217<br>V-73553<br>CCI-001849 (NIST SP 800-53 Rev 4: AU-4; NIST SP 800-53 Rev 5: AU-4) |
| Description: | 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. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1105<br>Result: false<br>Title: WN16-CC-000300<br>Description: The Application event log must be configured to 32768 KB or greater.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 32768 or higher) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:110500 (registry_test)<br>Result: false<br>Title: 'Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 32768 or higher<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:110500 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\EventLog\Application'<br>◦ name must be equal to 'MaxSize'<br>State ID: oval:mil.disa.stig.windows:ste:110500 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be greater than or equal to '32768'<br>Additional Information: Check existence requirement not met. |

### V-224938 - The Security event log size must be configured to 196608 KB or greater.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224938r877391_rule |
| Result: | Fail |
| Version: | WN16-CC-000310 |
| Identities: | CCE-44526-2<br>SV-88219<br>V-73555<br>CCI-001849 (NIST SP 800-53 Rev 4: AU-4; NIST SP 800-53 Rev 5: AU-4) |
| Description: | 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. false |
| Fix Text: | 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. |

| | |
|---|---|
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1106<br>Result: false<br>Title: WN16-CC-000310<br>Description: The Security event log must be configured to 196608 KB or greater.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 196608 or higher) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:110600 (registry_test)<br>Result: false<br>Title: 'Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 196608 or higher<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:110600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\EventLog\Security'<br>◦ name must be equal to 'MaxSize'<br>State ID: oval:mil.disa.stig.windows:ste:110600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be greater than or equal to '196608'<br>Additional Information: Check existence requirement not met. |

## V-224939 - The System event log size must be configured to 32768 KB or greater.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224939r877391_rule |
| Result: | Fail |
| Version: | WN16-CC-000320 |
| Identities: | CCE-46651-6<br>SV-88221<br>V-73557<br>CCI-001849 (NIST SP 800-53 Rev 4: AU-4; NIST SP 800-53 Rev 5: AU-4) |
| Description: | 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. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1107<br>Result: false<br>Title: WN16-CC-000320<br>Description: The System event log must be configured to 32768 KB or greater.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 32768 or higher) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:110700 (registry_test)<br>Result: false<br>Title: 'Specify the maximum log size (KB)' is set to 'Enabled' with 'Maximum Log Size (KB)' set to 32768 or higher<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:110700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\EventLog\System'<br>◦ name must be equal to 'MaxSize'<br>State ID: oval:mil.disa.stig.windows:ste:110700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be greater than or equal to '32768'<br>Additional Information: Check existence requirement not met. |

## V-224940 - Windows Server 2016 Windows SmartScreen must be enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224940r569186_rule |
| Result: | Fail |

| | |
|---|---|
| Version: | WN16-CC-000330 |
| Identities: | CCE-44884-5<br>V-73559<br>SV-88223<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | Windows SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling SmartScreen will warn users of potentially malicious programs. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> "Configure Windows SmartScreen" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1108<br>Result: false<br>Title: WN16-CC-000330<br>Description: Windows SmartScreen must be enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Configure Windows SmartScreen' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:110800 (registry_test)<br>Result: false<br>Title: 'Configure Windows SmartScreen' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:110800 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\System'<br>◦ name must be equal to 'EnableSmartScreen'<br>State ID: oval:mil.disa.stig.windows:ste:110800 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224944 - Passwords must not be saved in the Remote Desktop Client.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224944r852332_rule |
| Result: | Fail |
| Version: | WN16-CC-000370 |
| Identities: | CCE-44880-3<br>SV-88231<br>V-73567<br>CCI-002038 (NIST SP 800-53 Rev 4: IA-11) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1112<br>Result: false<br>Title: WN-16-CC-000370<br>Description: Passwords must not be saved in the Remote Desktop Client.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Do not allow passwords to be saved' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111200 (registry_test)<br>Result: false<br>Title: 'Do not allow passwords to be saved' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111200 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services'<br>◦ name must be equal to 'DisablePasswordSaving'<br>State ID: oval:mil.disa.stig.windows:ste:111200 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224945 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224945r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000380 |
| Identities: | CCE-46771-2<br>V-73569<br>SV-88233<br>CCI-001090 (NIST SP 800-53: SC-4; NIST SP 800-53A: SC-4.1; NIST SP 800-53 Rev 4: SC-4; NIST SP 800-53 Rev 5: SC-4) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1113<br>Result: false<br>Title: WN16-CC-000380<br>Description: Local drives must be prevented from sharing with Remote Desktop Session Hosts.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false ('Do not allow drive redirection' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111300 (registry_test)<br>Result: false<br>Title: 'Do not allow drive redirection' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111300 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows NT\Terminal Services'<br>◦ name must be equal to 'fDisableCdm'<br>State ID: oval:mil.disa.stig.windows:ste:111300 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224946 - Remote Desktop Services must always prompt a client for passwords upon connection.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224946r852333_rule |
| Result: | Fail |
| Version: | WN16-CC-000390 |
| Identities: | CCE-45743-2<br>SV-88235<br>V-73571<br>CCI-002038 (NIST SP 800-53 Rev 4: IA-11) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1114<br>Result: false<br>Title: WN16-CC-000390<br>Description: Remote Desktop Services must always prompt a client for passwords upon connection.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Always prompt for password upon connection' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111400 (registry_test)<br>Result: false<br>Title: 'Always prompt for password upon connection' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111400 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows NT\Terminal Services'<br>◦ name must be equal to 'fPromptForPassword'<br>State ID: oval:mil.disa.stig.windows:ste:111400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224947 - The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224947r877394_rule |
| Result: | Fail |
| Version: | WN16-CC-000400 |
| Identities: | CCE-44496-8<br>SV-88237<br>V-73573<br>CCI-001453 (NIST SP 800-53: AC-17 (2); NIST SP 800-53A: AC-17 (2).1; NIST SP 800-53 Rev 4: AC-17 (2); NIST SP 800-53 Rev 5: AC-17 (2)) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1115<br>Result: false<br>Title: WN16-CC-000400<br>Description: The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Require secure RPC communication' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111500 (registry_test)<br>Result: false<br>Title: 'Require secure RPC communication' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111500 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows NT\Terminal Services'<br>◦ name must be equal to 'fEncryptRPCTraffic'<br>State ID: oval:mil.disa.stig.windows:ste:111500 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224948 - Remote Desktop Services must be configured with the client connection encryption set to High Level.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224948r877394_rule |
| Result: | Fail |
| Version: | WN16-CC-000410 |
| Identities: | CCE-47193-8<br>SV-88239<br>V-73575<br>CCI-001453 (NIST SP 800-53: AC-17 (2); NIST SP 800-53A: AC-17 (2).1; NIST SP 800-53 Rev 4: AC-17 (2); NIST SP 800-53 Rev 5: AC-17 (2)) |
| Description: | 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. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1116<br>Result: false<br>Title: WN16-CC-000410<br>Description: Remote Desktop Services must be configured with the client connection encryption set to High Level.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Set client connection encryption level' is set to 'Enabled' with 'Encryption Level' set to 'High Level') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111600 (registry_test)<br>Result: false<br>Title: 'Set client connection encryption level' is set to 'Enabled' with 'Encryption Level' set to 'High Level'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows NT\Terminal Services'<br>◦ name must be equal to 'MinEncryptionLevel'<br>State ID: oval:mil.disa.stig.windows:ste:111600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '3'<br>Additional Information: Check existence requirement not met. |

## V-224949 - Attachments must be prevented from being downloaded from RSS feeds.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224949r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000420 |
| Identities: | CCE-45063-5<br>SV-88241<br>V-73577<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | Attachments from RSS feeds may not be secure. This setting will prevent attachments from being downloaded from RSS feeds. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> "Prevent downloading of enclosures" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1117<br>Result: false<br>Title: WN16-CC-000420<br>Description: Attachments must be prevented from being downloaded from RSS feeds.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Prevent downloading of enclosures' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111700 (registry_test)<br>Result: false<br>Title: 'Prevent downloading of enclosures' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111700 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Internet Explorer\Feeds'<br>◦ name must be equal to 'DisableEnclosureDownload'<br>State ID: oval:mil.disa.stig.windows:ste:111700 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224952 - Indexing of encrypted files must be turned off.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224952r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000440 |
| Identities: | V-73581<br>SV-88245<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | Indexing of encrypted files may expose sensitive data. This setting prevents encrypted files from being indexed. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Search >> "Allow indexing of encrypted files" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1262<br>Result: false<br>Title: Search - Encrypted Files Indexing<br>Description: Indexing of encrypted files must be turned off.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false ('Allow indexing of encrypted files' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:126200 (registry_test)<br>Result: false<br>Title: 'Allow indexing of encrypted files' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:126200 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\Windows Search'<br>◦ name must be equal to 'AllowIndexingEncryptedStoresOrItems'<br>State ID: oval:mil.disa.stig.windows:ste:126200 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224953 - Users must be prevented from changing installation options.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224953r852334_rule |
| Result: | Fail |
| Version: | WN16-CC-000450 |
| Identities: | CCE-46993-2<br>SV-88247<br>V-73583<br>CCI-001812 (NIST SP 800-53 Rev 4: CM-11 (2)) |
| Description: | Installation options for applications are typically controlled by administrators. This setting prevents users from changing installation options that may bypass security features. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Allow user control over installs" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1119<br>Result: false<br>Title: WN16-CC-000450<br>Description: Users must be prevented from changing installation options.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Enable user control over installs' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:111900 (registry_test)<br>Result: false<br>Title: 'Enable user control over installs' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:111900 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\Installer'<br>◦ name must be equal to 'EnableUserControl'<br>State ID: oval:mil.disa.stig.windows:ste:111900 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224957 - PowerShell script block logging must be enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224957r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000490 |
| Identities: | SV-88255<br>V-73591<br>CCI-000135 (NIST SP 800-53: AU-3 (1); NIST SP 800-53A: AU-3 (1).1 (ii); NIST SP 800-53 Rev 4: AU-3 (1); NIST SP 800-53 Rev 5: AU-3 (1)) |
| Description: | 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.<br><br>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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> "Turn on PowerShell Script Block Logging" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:137<br>Result: false<br>Title: PowerShell Script block logging must be enabled.<br>Description: PowerShell Script block logging must be enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Check if PowerShell Script Block Logging is set to enabled in the registry) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:13700 (registry_test)<br>Result: false<br>Title: Check if PowerShell Script Block Logging is set to enabled in the registry<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:13700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging'<br>◦ name must match the pattern 'EnableScriptBlockLogging'<br>State ID: oval:mil.disa.stig.windows:ste:13700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224959 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224959r877382_rule |
| Result: | Fail |

| | |
|---|---|
| Version: | WN16-CC-000510 |
| Identities: | CCE-46378-6<br>SV-88259<br>V-73595<br>CCI-002890 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6))<br>CCI-003123 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6)) |
| Description: | Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.<br><br>Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174 false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> "Allow unencrypted traffic" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1124<br>Result: false<br>Title: WN16-CC-000510<br>Description: The Windows Remote Management (WinRM) client must not allow unencrypted traffic.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('WinRM Client: Allow unencrypted traffic' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112400 (registry_test)<br>Result: false<br>Title: 'WinRM Client: Allow unencrypted traffic' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112400 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Client'<br>◦ name must be equal to 'AllowUnencryptedTraffic'<br>State ID: oval:mil.disa.stig.windows:ste:112400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

### V-224960 - The Windows Remote Management (WinRM) client must not use Digest authentication.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224960r877395_rule |
| Result: | Fail |
| Version: | WN16-CC-000520 |
| Identities: | CCE-46014-7<br>SV-88261<br>V-73597<br>CCI-000877 (NIST SP 800-53: MA-4 c; NIST SP 800-53A: MA-4.1 (iv); NIST SP 800-53 Rev 4: MA-4 c; NIST SP 800-53 Rev 5: MA-4 c) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Client >> "Disallow Digest authentication" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1125<br>Result: false<br>Title: WN16-CC-000520<br>Description: The Windows Remote Management (WinRM) client must not use Digest authentication.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Disallow Digest authentication' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112500 (registry_test)<br>Result: false<br>Title: 'Disallow Digest authentication' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112500 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Client'<br>◦ name must be equal to 'AllowDigest'<br>State ID: oval:mil.disa.stig.windows:ste:112500 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224962 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224962r877382_rule |
| Result: | Fail |
| Version: | WN16-CC-000540 |
| Identities: | CCE-45060-1<br>SV-88265<br>V-73601<br>CCI-002890 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6))<br>CCI-003123 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6)) |
| Description: | Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this.<br><br>Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174 false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> "Allow unencrypted traffic" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1127<br>Result: false<br>Title: WN16-CC-000540<br>Description: The Windows Remote Management (WinRM) service must not allow unencrypted traffic.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('WinRM Service: Allow unencrypted traffic' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112700 (registry_test)<br>Result: false<br>Title: 'WinRM Service: Allow unencrypted traffic' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Service'<br>◦ name must be equal to 'AllowUnencryptedTraffic'<br>State ID: oval:mil.disa.stig.windows:ste:112700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224963 - The Windows Remote Management (WinRM) service must not store RunAs credentials.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224963r852338_rule |
| Result: | Fail |
| Version: | WN16-CC-000550 |
| Identities: | CCE-46708-4<br>SV-88267<br>V-73603<br>CCI-002038 (NIST SP 800-53 Rev 4: IA-11) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1128<br>Result: false<br>Title: WN16-CC-000550<br>Description: The Windows Remote Management (WinRM) service must not store RunAs credentials.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Disallow WinRM from storing RunAs credentials' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:112800 (registry_test)<br>Result: false<br>Title: 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:112800 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Service'<br>◦ name must be equal to 'DisableRunAs'<br>State ID: oval:mil.disa.stig.windows:ste:112800 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

### V-225010 - Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225010r877039_rule |
| Result: | Fail |
| Version: | WN16-MS-000040 |
| Identities: | CCE-46880-1<br>SV-88203<br>V-73541<br>CCI-001967 (NIST SP 800-53 Rev 4: IA-3 (1); NIST SP 800-53 Rev 5: IA-3 (1)) |
| Description: | 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. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Procedure Call >> "Restrict Unauthenticated RPC clients" to "Enabled" with "Authenticated" selected. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1174<br>Result: false<br>Title: RPC - Unauthenticated RPC Clients<br>Description: Unauthenticated RPC clients must be restricted from connecting to the RPC server.<br>Class: compliance<br>Tests: ◦ false (One or more child checks must be true.)<br>▪ false ('Restrict Unauthenticated RPC clients' is set to 'Enabled' and 'Authenticated')<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:117400 (registry_test)<br>Result: false<br>Title: 'Restrict Unauthenticated RPC clients' is set to 'Enabled' and 'Authenticated'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:117400 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Windows NT\Rpc'<br>◦ name must be equal to 'RestrictRemoteClients'<br>State ID: oval:mil.disa.stig.windows:ste:117400 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)<br>Result: false<br>Title: System is a DC<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: One or more item-state comparisons may be true.<br>Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem'<br>State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '5'<br>State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '4'<br>Collected Item/State Result: [ false ]<br>◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT DomainRole FROM win32_computersystem'<br>◦ collected 'result' result:<br>▪ domainrole = '2'<br>Additional Information: Check requirement not met.<br>result |

## V-225013 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225013r877392_rule |
| Result: | Fail |
| Version: | WN16-MS-000310 |
| Identities: | CCE-45487-6<br>SV-88341<br>V-73677<br>CCI-002235 (NIST SP 800-53 Rev 4: AC-6 (10); NIST SP 800-53 Rev 5: AC-6 (10)) |
| Description: | The Windows Security Account Manager (SAM) stores users' passwords. Restricting Remote Procedure Call (RPC) connections to the SAM to Administrators helps protect those credentials. false |
| Fix Text: | 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".<br><br>Select "Edit Security" to configure the "Security descriptor:".<br><br>Add "Administrators" in "Group or user names:" if it is not already listed (this is the default).<br><br>Select "Administrators" in "Group or user names:".<br><br>Select "Allow" for "Remote Access" in "Permissions for "Administrators".<br><br>Click "OK".<br><br>The "Security descriptor:" must be populated with "O:BAG:BAD:(A;;RC;;;BA) for the policy to be enforced. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1210<br>Result: false<br>Title: Security Account Manager (SAM) RPC<br>Description: Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (Allow Administrators group to make remote calls to SAM)<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121000 (registry_test)<br>Result: false<br>Title: Allow Administrators group to make remote calls to SAM<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121000 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa'<br>◦ name must be equal to 'RestrictRemoteSAM'<br>State ID: oval:mil.disa.stig.windows:ste:121000 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_sz'<br>◦ check_existence = 'at_least_one_exists', value must be equal to 'O:BAG:BAD:(A;;RC;;;BA)'<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)<br>Result: false<br>Title: System is a DC<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: One or more item-state comparisons may be true.<br>Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem'<br>State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '5'<br>State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '4'<br>Collected Item/State Result:<br>◦ namespace equals 'root\cimv2'<br>[ false ]<br>◦ wql equals 'SELECT DomainRole FROM win32_computersystem'<br>◦ collected 'result' result:<br>▪ domainrole = '2'<br>Additional Information: Check requirement not met.<br>result |

## V-225014 - The "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on member servers.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225014r857272_rule |
| Result: | Fail |
| Version: | WN16-MS-000340 |
| Identities: | CCE-45486-8<br>SV-88397<br>V-73733<br>CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3; NIST SP 800-53 Rev 5: AC-3) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>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. false |
| Fix Text: | 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:<br><br>- Administrators<br>- Authenticated Users |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1176<br>Result: false<br>Title: WN16-MS-000340<br>Description: The Access this computer from the network user right must only be assigned to the Administrators and Authenticated User groups on member servers.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (Access this computer from the network - Administrators, Authenticated Users)<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:117600 (accesstoken_test)<br>Result: false<br>Title: Access this computer from the network - Administrators, Authenticated Users<br><br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:117601 (accesstoken_object)<br>Object Requirements: ◦ Collect any available items.<br>Exclude Items If: ◦ security_principle equals 'Administrators'<br>Exclude Items If: ◦ security_principle equals 'Authenticated Users'<br>State ID: oval:mil.disa.stig.windows:ste:117602 (accesstoken_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', senetworklogonright must be equal to '0'<br>Collected Item/State Result: ◦ senetworklogonright equals '1' for: Backup Operators, Everyone, Users<br>[ false ] ◦ senetworklogonright equals '0' for Remote Management Users, NETWORK SERVICE, Guests, Access Control Assistance Operators, System Managed Accounts Group, INTERACTIVE, CREATOR GROUP SERVER, NT SERVICE\ALL SERVICES, Power Users, TERMINAL SERVER USER, Performance Log Users, Cryptographic Operators, CREATOR GROUP, Administrator, RDS Management Servers, DIALUP, PROXY, Network Configuration Operators, RDS Endpoint Servers, IUSR, Remote Desktop Users, Hyper-V Administrators, LOCAL SERVICE, CREATOR OWNER SERVER, BATCH, NT SERVICE\WdiServiceHost, SERVICE, DefaultAccount, Replicator, Distributed COM Users, Event Log Readers, Guest, Print Operators, ANONYMOUS LOGON, Storage Replica Administrators, ENTERPRISE DOMAIN CONTROLLERS, Certificate Service DCOM Access, CREATOR OWNER, NETWORK, Performance Monitor Users, IIS_IUSRS, SYSTEM, RDS Remote Access Servers<br>Additional Information: Check requirement not met.<br>senetworklogonright<br>senetworklogonright<br>senetworklogonright<br><br>Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)<br>Result: false<br>Title: System is a DC<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: One or more item-state comparisons may be true.<br>Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)<br>Object Requirements: ◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem'<br>State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)<br>State Requirements: ◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '5'<br>State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)<br>State Requirements: ◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '4'<br>Collected Item/State Result: ◦ namespace equals 'root\cimv2'<br>[ false ] ◦ wql equals 'SELECT DomainRole FROM win32_computersystem'<br>◦ collected 'result' result:<br>▪ domainrole = '2'<br>Additional Information: Check requirement not met.<br>result |

## V-225015 - 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.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225015r857274_rule |
| Result: | Fail |
| Version: | WN16-MS-000370 |
| Identities: | CCE-44499-2<br>V-73759<br>SV-88423<br>CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3; NIST SP 800-53 Rev 5: AC-3) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>The "Deny access to this computer from the network" user right defines the accounts that are prevented from logging on from the network.<br><br>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.<br><br>Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.<br><br>The Guests group must be assigned this right to prevent unauthenticated access. false |
| Fix Text: | 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:<br><br>Domain Systems Only:<br>- Enterprise Admins group<br>- Domain Admins group<br>- "Local account and member of Administrators group" or "Local account" (see Note below)<br><br>All Systems:<br>- Guests group<br><br>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. |
| Severity: | medium |
| Weight: | 10.0 |

**Reference:**

Title: DPMS Target Microsoft Windows Server 2016
Publisher: DISA
Type: DPMS Target
Subject: Microsoft Windows Server 2016
Identifier: 4205

**Definitions:**

Definition ID: oval:mil.disa.stig.windows:def:1177
Result: false
Title: WN16-MS-000370
Description: 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.
Class: compliance
Tests:
- false (One or more child checks must be true.)
  - false (All child checks must be true.)
    - true (System is a standalone server)
    - false (Deny access to this computer from the network - Guests)
  - false (All child checks must be true.)
    - false (One or more child checks must be true.)
      - false (Deny access to this computer from the network - Local account)
      - false (Deny access to this computer from the network - Local account and member of Administrators group)
    - false (Deny access to this computer from the network - Guests)
    - false (Deny access to this computer from the network - Domain Admins)
    - false (Deny access to this computer from the network - Enterprise Admins)
    - false (All child checks must be true.)
      - false (System is a member server)
  - false (All child checks must be true.)
    - false (System is a DC)

**Tests:**

Test ID: oval:mil.disa.stig.windows:tst:117705 (wmi57_test)
Result: true
Title: System is a standalone server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117701 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '2'

---

Test ID: oval:mil.disa.stig.windows:tst:117700 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Guests
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117700 (accesstoken_object)
Object Requirements:
- security_principle must be equal to 'Guests'

State ID: oval:mil.disa.stig.windows:ste:117700 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenynetworklogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenynetworklogonright equals '1' for:
- sedenynetworklogonright equals '0' for Guests

Additional Information: Check requirement not met.
sedenynetworklogonright

---

Test ID: oval:mil.disa.stig.windows:tst:117703 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Local account
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117705 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:117700 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenynetworklogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenynetworklogonright equals '1' for:
- sedenynetworklogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117704 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Local account and member of Administrators group
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117708 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:117700 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenynetworklogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenynetworklogonright equals '1' for:
- sedenynetworklogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117701 (accesstoken_test)
Result: false
Title: Deny access to this computer from the network - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117701 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:117700 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenynetworklogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenynetworklogonright equals '1' for:
- sedenynetworklogonright equals '0' for

| | |
|---|---|
| Additional Information: | Check existence requirement not met. |

| | |
|---|---|
| Test ID: | oval:mil.disa.stig.windows:tst:117702 (accesstoken_test) |
| Result: | false |
| Title: | Deny access to this computer from the network - Enterprise Admins |
| Check Existence: | One or more collected items must exist. |
| Check: | At least one collected item must match the given state(s). |
| Object ID: | oval:mil.disa.stig.windows:obj:117702 (accesstoken_object) |
| Object Requirements: | ◦ Collect any available items. |
| State ID: | oval:mil.disa.stig.windows:ste:117700 (accesstoken_state) |
| State Requirements: | ◦ check_existence = 'at_least_one_exists', sedenynetworklogonright must be equal to '1' |
| Collected Item/State Result: [ false ] | ◦ sedenynetworklogonright equals '1' for:<br>◦ sedenynetworklogonright equals '0' for |
| Additional Information: | Check existence requirement not met. |

| | |
|---|---|
| Test ID: | oval:mil.disa.stig.windows:tst:117100 (wmi57_test) |
| Result: | false |
| Title: | System is a member server |
| Check Existence: | One or more collected items must exist. |
| Check: | All collected items must match the given state(s). |
| Object ID: | oval:mil.disa.stig.windows:obj:101000 (wmi57_object) |
| Object Requirements: | ◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem' |
| State ID: | oval:mil.disa.stig.windows:ste:117100 (wmi57_state) |
| State Requirements: | ◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '3' |
| Collected Item/State Result: [ false ] | ◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT DomainRole FROM win32_computersystem'<br>◦ collected 'result' result:<br>▪ domainrole = '2' |
| Additional Information: | Check requirement not met.<br>result |

| | |
|---|---|
| Test ID: | oval:mil.disa.stig.windows:tst:101000 (wmi57_test) |
| Result: | false |
| Title: | System is a DC |
| Check Existence: | One or more collected items must exist. |
| Check: | All collected items must match the given state(s). |
| State Operator: | One or more item-state comparisons may be true. |
| Object ID: | oval:mil.disa.stig.windows:obj:101000 (wmi57_object) |
| Object Requirements: | ◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem' |
| State ID: | oval:mil.disa.stig.windows:ste:101000 (wmi57_state) |
| State Requirements: | ◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '5' |
| State ID: | oval:mil.disa.stig.windows:ste:101001 (wmi57_state) |
| State Requirements: | ◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '4' |
| Collected Item/State Result: [ false ] | ◦ namespace equals 'root\cimv2'<br>◦ wql equals 'SELECT DomainRole FROM win32_computersystem'<br>◦ collected 'result' result:<br>▪ domainrole = '2' |
| Additional Information: | Check requirement not met.<br>result |

## V-225016 - 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.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225016r857276_rule |
| Result: | Fail |
| Version: | WN16-MS-000380 |
| Identities: | CCE-47287-8<br>V-73763<br>SV-88427<br>CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3; NIST SP 800-53 Rev 5: AC-3) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>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.<br><br>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.<br><br>The Guests group must be assigned to prevent unauthenticated access. false |
| Fix Text: | 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:<br><br>Domain Systems Only:<br>- Enterprise Admins Group<br>- Domain Admins Group<br><br>All Systems:<br>- Guests Group |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1178<br>Result: false<br>Title: UR: Deny log on as a batch job - Member Server<br>Description: 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 unauthenticated access on all systems.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ true (System is a standalone server)<br>▪ false (Deny log on as a batch job - Guests)<br>▪ false (All child checks must be true.)<br>▪ false (Deny log on as a batch job - Guests)<br>▪ false (Deny log on as a batch job - Domain Admins)<br>▪ false (Deny log on as a batch job - Enterprise Admins)<br>▪ false (All child checks must be true.)<br>▪ false (System is a member server)<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |

Tests:

Test ID: oval:mil.disa.stig.windows:tst:117705 (wmi57_test)
Result: true
Title: System is a standalone server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117701 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '2'

---

Test ID: oval:mil.disa.stig.windows:tst:117800 (accesstoken_test)
Result: false
Title: Deny log on as a batch job - Guests
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117700 (accesstoken_object)
Object Requirements:
- security_principle must be equal to 'Guests'

State ID: oval:mil.disa.stig.windows:ste:117800 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenybatchLogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenybatchLogonright equals '1' for:
- sedenybatchLogonright equals '0' for Guests

Additional Information: Check requirement not met.
sedenybatchLogonright

---

Test ID: oval:mil.disa.stig.windows:tst:117801 (accesstoken_test)
Result: false
Title: Deny log on as a batch job - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117701 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:117800 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenybatchLogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenybatchLogonright equals '1' for:
- sedenybatchLogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117802 (accesstoken_test)
Result: false
Title: Deny log on as a batch job - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117702 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:117800 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenybatchLogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenybatchLogonright equals '1' for:
- sedenybatchLogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117100 (wmi57_test)
Result: false
Title: System is a member server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117100 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '3'

Collected Item/State Result: [ false ]
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

---

Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)
Result: false
Title: System is a DC
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
State Operator: One or more item-state comparisons may be true.
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '5'

State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '4'

Collected Item/State Result: [ false ]
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

## V-225018 - 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.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225018r857278_rule |
| Result: | Fail |
| Version: | WN16-MS-000400 |
| Identities: | CCE-46108-7<br>V-73771<br>SV-88435<br>CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3; NIST SP 800-53 Rev 5: AC-3) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>The "Deny log on locally" user right defines accounts that are prevented from logging on interactively.<br><br>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.<br><br>The Guests group must be assigned this right to prevent unauthenticated access. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> "Deny log on locally" to include the following:<br><br>Domain Systems Only:<br>- Enterprise Admins Group<br>- Domain Admins Group<br><br>All Systems:<br>- Guests Group |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1180<br>Result: false<br>Title: Deny log on locally - Member and Standalone Server<br>Description: 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 unauthenticated access on all systems.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ true (System is a standalone server)<br>▪ false (Deny log on locally - Guests)<br>▪ false (All child checks must be true.)<br>▪ false (Deny log on locally - Guests)<br>▪ false (Deny log on locally - Domain Admins)<br>▪ false (Deny log on as a locally - Enterprise Admins)<br>▪ false (All child checks must be true.)<br>▪ false (System is a member server)<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |

Tests:

Test ID: oval:mil.disa.stig.windows:tst:117705 (wmi57_test)
Result: true
Title: System is a standalone server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117701 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '2'

---

Test ID: oval:mil.disa.stig.windows:tst:118000 (accesstoken_test)
Result: false
Title: Deny log on locally - Guests
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).

Object ID: oval:mil.disa.stig.windows:obj:117700 (accesstoken_object)
Object Requirements:
- security_principle must be equal to 'Guests'

State ID: oval:mil.disa.stig.windows:ste:118000 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyinteractivelogonright must be equal to '1'

Collected Item/State Result [ false ]:
- sedenyinteractivelogonright equals '1' for:
- sedenyinteractivelogonright equals '0' for Guests

Additional Information: Check requirement not met.
sedenyinteractivelogonright

---

Test ID: oval:mil.disa.stig.windows:tst:118001 (accesstoken_test)
Result: false
Title: Deny log on locally - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117701 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:118000 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyinteractivelogonright must be equal to '1'

Collected Item/State Result [ false ]:
- sedenyinteractivelogonright equals '1' for:
- sedenyinteractivelogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:118002 (accesstoken_test)
Result: false
Title: Deny log on as a locally - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117702 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:118000 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyinteractivelogonright must be equal to '1'

Collected Item/State Result [ false ]:
- sedenyinteractivelogonright equals '1' for:
- sedenyinteractivelogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117100 (wmi57_test)
Result: false
Title: System is a member server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117100 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '3'

Collected Item/State Result [ false ]:
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

---

Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)
Result: false
Title: System is a DC
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
State Operator: One or more item-state comparisons may be true.
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '5'

State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '4'

Collected Item/State Result [ false ]:
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

## V-225019 - 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.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225019r860023_rule |
| Result: | Fail |
| Version: | WN16-MS-000410 |
| Identities: | CCE-47279-5<br>SV-88439<br>V-73775<br>CCI-002314 (NIST SP 800-53 Rev 4: AC-17 (1); NIST SP 800-53 Rev 5: AC-17 (1)) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>The "Deny log on through Remote Desktop Services" user right defines the accounts that are prevented from logging on using Remote Desktop Services.<br><br>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.<br><br>Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.<br><br>The Guests group must be assigned this right to prevent unauthenticated access. false |
| Fix Text: | 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:<br><br>Domain Systems Only:<br>- Enterprise Admins group<br>- Domain Admins group<br>- Local account (see Note below)<br><br>All Systems:<br>- Guests group<br><br>Note: "Local account" is referring to the Windows built-in security group. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1181<br>Result: false<br>Title: Deny log on through Remote Desktop Services - Member and Standalone Servers<br>Description: 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 local administrator accounts on domain systems and unauthenticated access on all systems.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ true (System is a standalone server)<br>▪ false (Deny log on through Remote Desktop Services - Guests)<br>▪ false (All child checks must be true.)<br>▪ false (Deny log on through Remote Desktop Services - Guests)<br>▪ false (Deny log on through Remote Desktop Services - Domain Admins)<br>▪ false (Deny log on through Remote Desktop Services - Enterprise Admins)<br>▪ false (Deny log on through Remote Desktop Services - Local account)<br>▪ false (All child checks must be true.)<br>▪ false (System is a member server)<br>▪ false (All child checks must be true.)<br>▪ false (System is a DC) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:117705 (wmi57_test)<br>Result: true<br>Title: System is a standalone server<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)<br>Object Requirements:<br>◦ namespace must be equal to 'root\cimv2'<br>◦ wql must be equal to 'SELECT DomainRole FROM win32_computersystem'<br>State ID: oval:mil.disa.stig.windows:ste:117701 (wmi57_state)<br>State Requirements:<br>◦ for all 'result' the following must be true:<br>▪ all domainrole must be equal to '2'<br><br>Test ID: oval:mil.disa.stig.windows:tst:118100 (accesstoken_test)<br>Result: false<br>Title: Deny log on through Remote Desktop Services - Guests<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:117700 (accesstoken_object)<br>Object Requirements:<br>◦ security_principle must be equal to 'Guests'<br>State ID: oval:mil.disa.stig.windows:ste:118100 (accesstoken_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', sedenyremoteInteractivelogonright must be equal to '1'<br>Collected Item/State Result: [ false ]<br>◦ sedenyremoteInteractivelogonright equals '1' for:<br>◦ sedenyremoteInteractivelogonright equals '0' for Guests |

Additional Information: Check requirement not met.
sedenyremoteInteractivelogonright

---

Test ID: oval:mil.disa.stig.windows:tst:118101 (accesstoken_test)
Result: false
Title: Deny log on through Remote Desktop Services - Domain Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117701 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:118100 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyremoteInteractivelogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenyremoteInteractivelogonright equals '1' for:
- sedenyremoteInteractivelogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:118102 (accesstoken_test)
Result: false
Title: Deny log on through Remote Desktop Services - Enterprise Admins
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117702 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:118100 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyremoteInteractivelogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenyremoteInteractivelogonright equals '1' for:
- sedenyremoteInteractivelogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:118103 (accesstoken_test)
Result: false
Title: Deny log on through Remote Desktop Services - Local account
Check Existence: One or more collected items must exist.
Check: At least one collected item must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:117705 (accesstoken_object)
Object Requirements:
- Collect any available items.

State ID: oval:mil.disa.stig.windows:ste:118100 (accesstoken_state)
State Requirements:
- check_existence = 'at_least_one_exists', sedenyremoteInteractivelogonright must be equal to '1'

Collected Item/State Result: [ false ]
- sedenyremoteInteractivelogonright equals '1' for:
- sedenyremoteInteractivelogonright equals '0' for

Additional Information: Check existence requirement not met.

---

Test ID: oval:mil.disa.stig.windows:tst:117100 (wmi57_test)
Result: false
Title: System is a member server
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:117100 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '3'

Collected Item/State Result: [ false ]
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

---

Test ID: oval:mil.disa.stig.windows:tst:101000 (wmi57_test)
Result: false
Title: System is a DC
Check Existence: One or more collected items must exist.
Check: All collected items must match the given state(s).
State Operator: One or more item-state comparisons may be true.
Object ID: oval:mil.disa.stig.windows:obj:101000 (wmi57_object)
Object Requirements:
- namespace must be equal to 'root\cimv2'
- wql must be equal to 'SELECT DomainRole FROM win32_computersystem'

State ID: oval:mil.disa.stig.windows:ste:101000 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '5'

State ID: oval:mil.disa.stig.windows:ste:101001 (wmi57_state)
State Requirements:
- for all 'result' the following must be true:
  - all domainrole must be equal to '4'

Collected Item/State Result: [ false ]
- namespace equals 'root\cimv2'
- wql equals 'SELECT DomainRole FROM win32_computersystem'
- collected 'result' result:
  - domainrole = '2'

Additional Information: Check requirement not met.
result

## V-225021 - The DoD Root CA certificates must be installed in the Trusted Root Store.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225021r890508_rule |
| Result: | Fail |
| Version: | WN16-PK-000010 |

| | |
|---|---|
| Identities: | SV-88269<br>V-73605<br>CCI-000185 (NIST SP 800-53: IA-5 (2); NIST SP 800-53A: IA-5 (2).1; NIST SP 800-53 Rev 4: IA-5 (2) (a); NIST SP 800-53 Rev 5: IA-5 (2) (b) (1))<br>CCI-002470 (NIST SP 800-53 Rev 4: SC-23 (5); NIST SP 800-53 Rev 5: SC-23 (5)) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182 false |
| Fix Text: | Install the DoD Root CA certificates:<br>DoD Root CA 3<br>DoD Root CA 4<br>DoD Root CA 5<br><br>The InstallRoot tool is available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:225021<br>Result: false<br>Title: WN16-PK-000010 - The DoD Root CA certificates must be installed in the Trusted Root Store.<br>Description: 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (The DoD Root CA 3 Certificate expiring 12/30/2029 is installed into the Trusted Root Store.)<br>▪ false (The DoD Root CA 4 Certificate expiring 7/25/2032 is installed into the Trusted Root Store.)<br>▪ false (The DoD Root CA 5 Certificate expiring 6/14/2041 is installed into the Trusted Root Store.) |
| Tests: | Test ID: oval:mil.disa.stig.win:tst:25342700 (registry_test)<br>Result: false<br>Title: The DoD Root CA 3 Certificate expiring 12/30/2029 is installed into the Trusted Root Store.<br>Check Existence: One or more collected items must exist.<br>Check: Result is based on check existence only.<br>Object ID: oval:mil.disa.stig.win:obj:25342700 (registry_object)<br>Object Requirements: ◦ Collect any available items.<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.win:tst:25342701 (registry_test)<br>Result: false<br>Title: The DoD Root CA 4 Certificate expiring 7/25/2032 is installed into the Trusted Root Store.<br>Check Existence: One or more collected items must exist.<br>Check: Result is based on check existence only.<br>Object ID: oval:mil.disa.stig.win:obj:25342705 (registry_object)<br>Object Requirements: ◦ Collect any available items.<br>Additional Information: Check existence requirement not met.<br><br>Test ID: oval:mil.disa.stig.win:tst:25342702 (registry_test)<br>Result: false<br>Title: The DoD Root CA 5 Certificate expiring 6/14/2041 is installed into the Trusted Root Store.<br>Check Existence: One or more collected items must exist.<br>Check: Result is based on check existence only.<br>Object ID: oval:mil.disa.stig.win:obj:25342710 (registry_object)<br>Object Requirements: ◦ Collect any available items.<br>Additional Information: Check existence requirement not met. |

## V-225022 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225022r894338_rule |
| Result: | Fail |
| Version: | WN16-PK-000020 |
| Identities: | SV-88271<br>V-73607<br>CCI-000185 (NIST SP 800-53: IA-5 (2); NIST SP 800-53A: IA-5 (2).1; NIST SP 800-53 Rev 4: IA-5 (2) (a); NIST SP 800-53 Rev 5: IA-5 (2) (b) (1))<br>CCI-002440 (NIST SP 800-53 Rev 4: SC-12; NIST SP 800-53 Rev 5: SC-12) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182 false |

| | |
|---|---|
| Fix Text: | Install the DoD Interoperability Root CA cross-certificates on unclassified systems.<br><br>Issued To - Issued By - Thumbprint<br>DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477<br><br>The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:225022<br>Result: false<br>Title: WN16-PK-000020 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.<br>Description: 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (DoD Interoperability Root CA 2 certificate expiring 11/16/2024 is installed in the Untrusted Certificates Store) |
| Tests: | Test ID: oval:mil.disa.stig.win:tst:25342900 (registry_test)<br>Result: false<br>Title: DoD Interoperability Root CA 2 certificate expiring 11/16/2024 is installed in the Untrusted Certificates Store<br>Check Existence: One or more collected items must exist.<br>Check: Result is based on check existence only.<br>Object ID: oval:mil.disa.stig.win:obj:25342900 (registry_object)<br>Object Requirements: ◦ Collect any available items.<br>Additional Information: Check existence requirement not met. |

## V-225023 - The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225023r890514_rule |
| Result: | Fail |
| Version: | WN16-PK-000030 |
| Identities: | V-73609<br>SV-88273<br>CCI-000185 (NIST SP 800-53: IA-5 (2); NIST SP 800-53A: IA-5 (2).1; NIST SP 800-53 Rev 4: IA-5 (2) (a); NIST SP 800-53 Rev 5: IA-5 (2) (b) (1))<br>CCI-002470 (NIST SP 800-53 Rev 4: SC-23 (5); NIST SP 800-53 Rev 5: SC-23 (5)) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182 false |
| Fix Text: | Install the US DoD CCEB Interoperability Root CA cross-certificate on unclassified systems.<br><br>Subject: CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U.S. Government, C=US<br>Issuer: CN=US DoD CCEB Interoperability Root CA 2, OU=PKI, OU=DoD, O=U.S. Government, C=US<br>Thumbprint: 9B74964506C7ED9138070D08D5F8B969866560C8<br>NotAfter: 7/18/2025<br><br>The certificates can be installed using the InstallRoot tool. The tool and user guide are available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. Certificate bundles published by the PKI can be found at https://crl.gds.disa.mil/. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |

| | |
|---|---|
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:225023<br>Result: false<br>Title: WN16-PK-000030 - The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.<br>Description: 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.<br><br>Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (US DoD CCEB Interoperability Root CA 2 cross-certificate expiring 7/18/2025 is installed in the Untrusted Certificates Store) |
| Tests: | Test ID: oval:mil.disa.stig.win:tst:25343000 (registry_test)<br>Result: false<br>Title: US DoD CCEB Interoperability Root CA 2 cross-certificate expiring 7/18/2025 is installed in the Untrusted Certificates Store<br>Check Existence: One or more collected items must exist.<br>Check: Result is based on check existence only.<br>Object ID: oval:mil.disa.stig.win:obj:25343000 (registry_object)<br>Object Requirements: ◦ Collect any available items.<br>Additional Information: Check existence requirement not met. |

## V-225026 - Windows Server 2016 built-in administrator account must be renamed.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225026r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000030 |
| Identities: | CCE-46321-6<br>SV-88287<br>V-73623<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1185<br>Result: false<br>Title: Rename Built-in Administrator Account<br>Description: The built-in administrator account must be renamed.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Accounts: Rename administrator account' is not set to 'Administrator')<br>▪ true ('Accounts: Rename administrator account' is not set to 'localdomain\Administrator') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:118500 (sid_sid_test)<br>Result: false<br>Title: 'Accounts: Rename administrator account' is not set to 'Administrator'<br>Check Existence: Zero or more collected items may exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:118500 (sid_sid_object)<br>Object Requirements: ◦ trustee_sid must match the pattern '^S-1-5-[0-9-]+-500$'<br>State ID: oval:mil.disa.stig.windows:ste:118500 (sid_sid_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', trustee_name must not be equal (case insensitive) to 'Administrator'<br>Collected Item/State Result: [ false ] ◦ trustee_sid equals 'S-1-5-21-576533568-2147367016-1630951814-500'<br>◦ trustee_name equals 'Administrator'<br>◦ trustee_domain equals 'WIN-4FBN6UUD6B0'<br>Additional Information: Check requirement not met.<br>trustee_name<br><br>Test ID: oval:mil.disa.stig.windows:tst:118501 (sid_sid_test)<br>Result: true<br>Title: 'Accounts: Rename administrator account' is not set to 'localdomain\Administrator'<br>Check Existence: Zero or more collected items may exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:118500 (sid_sid_object)<br>Object Requirements: ◦ trustee_sid must match the pattern '^S-1-5-[0-9-]+-500$'<br>State ID: oval:mil.disa.stig.windows:ste:118501 (sid_sid_state)<br>State Requirements: ◦ for check = 'all', trustee_name, the following must be true:<br>▪ trustee_name must not be equal (case insensitive) to 'WIN-4FBN6UUD6B0\Administrator' |

## V-225027 - Windows Server 2016 built-in guest account must be renamed.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225027r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000040 |
| Identities: | CCE-46218-4<br>SV-88289<br>V-73625<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1186<br>Result: false<br>Title: Rename Built-in Guest Account<br>Description: The built-in guest account must be renamed.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Accounts: Rename Guest account' is not set to 'Guest')<br>▪ true ('Accounts: Rename Guest account' is not set to 'localdomain\Guest') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:118600 (sid_sid_test)<br>Result: false<br>Title: 'Accounts: Rename Guest account' is not set to 'Guest'<br>Check Existence: Zero or more collected items may exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:118600 (sid_sid_object)<br>Object Requirements: ◦ trustee_sid must match the pattern '^S-1-5-[0-9-]+-501$'<br>State ID: oval:mil.disa.stig.windows:ste:118600 (sid_sid_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', trustee_name must not be equal (case insensitive) to 'Guest'<br>Collected Item/State Result: ◦ trustee_sid equals 'S-1-5-21-576533568-2147367016-1630951814-501'<br>[ false ] ◦ trustee_name equals 'Guest'<br>◦ trustee_domain equals 'WIN-4FBN6UUD6B0'<br>Additional Information: Check requirement not met.<br>trustee_name<br><br>Test ID: oval:mil.disa.stig.windows:tst:118601 (sid_sid_test)<br>Result: true<br>Title: 'Accounts: Rename Guest account' is not set to 'localdomain\Guest'<br>Check Existence: Zero or more collected items may exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:118600 (sid_sid_object)<br>Object Requirements: ◦ trustee_sid must match the pattern '^S-1-5-[0-9-]+-501$'<br>State ID: oval:mil.disa.stig.windows:ste:118601 (sid_sid_state)<br>State Requirements: ◦ for check = 'all', trustee_name, the following must be true:<br>▪ trustee_name must not be equal (case insensitive) to 'WIN-4FBN6UUD6B0\Guest' |

## V-225028 - Audit policy using subcategories must be enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225028r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000050 |
| Identities: | CCE-46406-5<br>SV-88291<br>V-73627<br>CCI-000169 (NIST SP 800-53: AU-12 a; NIST SP 800-53A: AU-12.1 (ii); NIST SP 800-53 Rev 4: AU-12 a; NIST SP 800-53 Rev 5: AU-12 a) |
| Description: | 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.<br>This setting allows administrators to enable more precise auditing capabilities. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1187<br>Result: false<br>Title: Audit policy using subcategories must be enabled<br>Description: Audit policy using subcategories must be enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:118700 (registry_test)<br>Result: false<br>Title: 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:118700 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa'<br>◦ name must be equal to 'SCENoApplyLegacyAuditPolicy'<br>State ID: oval:mil.disa.stig.windows:ste:118700 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

### V-225035 - The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225035r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000140 |
| Identities: | V-73645<br>SV-88309<br>CCI-000057 (NIST SP 800-53: AC-11 a; NIST SP 800-53A: AC-11.1 (ii); NIST SP 800-53 Rev 4: AC-11 a; NIST SP 800-53 Rev 5: AC-11 a) |
| Description: | 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. false |
| Fix Text: | 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. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows2016:def:225035<br>Result: false<br>Title: WN16-SO-000140 - The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.<br>Description: 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.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (The machine inactivity limit is set to 15 minutes or less) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:25344400 (registry_test)<br>Result: false<br>Title: The machine inactivity limit is set to 15 minutes or less<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>State Operator: All item-state comparisons must be true.<br>Object ID: oval:mil.disa.stig.windows:obj:25344400 (registry_object)<br>Object Requirements: ◦ hive must be equal (case insensitive) to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal (case insensitive) to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name must be equal (case insensitive) to 'InactivityTimeoutSecs'<br>State ID: oval:mil.disa.stig.windows:ste:25344400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be less than or equal to '900'<br>State ID: oval:mil.disa.stig.windows:ste:25344401 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be greater than '0'<br>Additional Information: Check existence requirement not met. |

### V-225038 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225038r569186_rule |

| | |
|---|---|
| Result: | Fail |
| Version: | WN16-SO-000180 |
| Identities: | CCE-46148-3<br>SV-88473<br>V-73807<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1197<br>Result: false<br>Title: Smart Card Removal Option<br>Description: The Smart Card removal option must be configured to Force Logoff or Lock Workstation.<br>Class: compliance<br>Tests:<br>◦ false (One or more child checks must be true.)<br>▪ false ('Interactive logon: Smart card removal behavior' is set to 'Lock Workstation')<br>▪ false ('Interactive logon: Smart card removal behavior' is set to 'Force Logoff') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:119700 (registry_test)<br>Result: false<br>Title: 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:119700 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon'<br>◦ name must be equal to 'scremoveoption'<br>State ID: oval:mil.disa.stig.windows:ste:119700 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_sz'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon'<br>◦ name equals 'scremoveoption'<br>◦ last_write_time equals '133302866960000000'<br>◦ type equals 'reg_sz'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.stig.windows:tst:119701 (registry_test)<br>Result: false<br>Title: 'Interactive logon: Smart card removal behavior' is set to 'Force Logoff'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:119700 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon'<br>◦ name must be equal to 'scremoveoption'<br>State ID: oval:mil.disa.stig.windows:ste:119701 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_sz'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '2'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon'<br>◦ name equals 'scremoveoption'<br>◦ last_write_time equals '133302866960000000'<br>◦ type equals 'reg_sz'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

### V-225039 - The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225039r852383_rule |
| Result: | Fail |
| Version: | WN16-SO-000190 |
| Identities: | CCE-46135-0<br>SV-88317<br>V-73653<br>CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8)<br>CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1)) |

| | |
|---|---|
| Description: | 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.<br><br>Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Microsoft network client: Digitally sign communications (always)" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1198<br>Result: false<br>Title: SMB Client Packet Signing (Always)<br>Description: The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Microsoft Network Client: Digitally sign communications (always)' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:119800 (registry_test)<br>Result: false<br>Title: 'Microsoft Network Client: Digitally sign communications (always)' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:119800 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Services\LanmanWorkstation\Parameters'<br>◦ name must be equal to 'RequireSecuritySignature'<br>State ID: oval:mil.disa.stig.windows:ste:119800 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: [ false ] ◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'System\CurrentControlSet\Services\LanmanWorkstation\Parameters'<br>◦ name equals 'RequireSecuritySignature'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

## V-225042 - The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225042r852385_rule |
| Result: | Fail |
| Version: | WN16-SO-000230 |
| Identities: | CCE-47038-5<br>SV-88325<br>V-73661<br>CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8)<br>CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1)) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Microsoft network server: Digitally sign communications (always)" to "Enabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1202<br>Result: false<br>Title: The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.<br>Description: The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Microsoft network server: Digitally sign communications (always)' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:120200 (registry_test)<br>Result: false<br><br>Title: 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:120200 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\LanManServer\Parameters'<br>◦ name must be equal to 'RequireSecuritySignature'<br>State ID: oval:mil.disa.stig.windows:ste:120200 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: ◦ hive equals 'HKEY_LOCAL_MACHINE'<br>[ false ] ◦ key equals 'SYSTEM\CurrentControlSet\Services\LanManServer\Parameters'<br>◦ name equals 'RequireSecuritySignature'<br>◦ last_write_time equals '133302938290000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

### V-225043 - The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225043r852386_rule |
| Result: | Fail |
| Version: | WN16-SO-000240 |
| Identities: | CCE-46230-9<br>SV-88327<br>V-73663<br>CCI-002418 (NIST SP 800-53 Rev 4: SC-8; NIST SP 800-53 Rev 5: SC-8)<br>CCI-002421 (NIST SP 800-53 Rev 4: SC-8 (1); NIST SP 800-53 Rev 5: SC-8 (1)) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1203<br>Result: false<br>Title: The Setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.<br>Description: The Setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:120300 (registry_test)<br>Result: false<br>Title: 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:120300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Services\LanManServer\Parameters'<br>◦ name must be equal to 'EnableSecuritySignature'<br>State ID: oval:mil.disa.stig.windows:ste:120300 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: ◦ hive equals 'HKEY_LOCAL_MACHINE'<br>[ false ] ◦ key equals 'SYSTEM\CurrentControlSet\Services\LanManServer\Parameters'<br>◦ name equals 'EnableSecuritySignature'<br>◦ last_write_time equals '133302938290000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

### V-225049 - Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225049r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000320 |
| Identities: | CCE-46338-0<br>SV-88343<br>V-73679<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1211<br>Result: false<br>Title: Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.<br>Description: Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network Security: Allow Local System to use computer identity for NTLM' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121100 (registry_test)<br>Result: false<br>Title: 'Network Security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121100 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa'<br>◦ name must be equal to 'UseMachineId'<br>State ID: oval:mil.disa.stig.windows:ste:121100 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

### V-225050 - NTLM must be prevented from falling back to a Null session.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225050r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000330 |
| Identities: | CCE-47296-9<br>SV-88345<br>V-73681<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Network security: Allow LocalSystem NULL session fallback" to "Disabled". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1212<br>Result: false<br>Title: NTLM must be prevented from falling back to a Null session.<br>Description: NTLM must be prevented from falling back to a Null session.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121200 (registry_test)<br>Result: false<br>Title: 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121200 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name must be equal to 'allownullsessionfallback'<br>State ID: oval:mil.disa.stig.windows:ste:121200 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-225051 - PKU2U authentication using online identities must be prevented.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225051r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000340 |
| Identities: | CCE-46030-3<br>SV-88347<br>V-73683<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1213<br>Result: false<br>Title: PKU2U authentication using online identities must be prevented.<br>Description: PKU2U authentication using online identities must be prevented.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121300 (registry_test)<br>Result: false<br>Title: 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\LSA\pku2u'<br>◦ name must be equal to 'AllowOnlineID'<br>State ID: oval:mil.disa.stig.windows:ste:121300 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-225052 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225052r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000350 |
| Identities: | CCE-44602-1<br>V-73685<br>SV-88349<br>CCI-000803 (NIST SP 800-53: IA-7; NIST SP 800-53A: IA-7.1; NIST SP 800-53 Rev 4: IA-7; NIST SP 800-53 Rev 5: IA-7) |
| Description: | Certain encryption types are no longer considered secure. The DES and RC4 encryption suites must not be used for Kerberos encryption.<br><br>Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting "The other domain supports Kerberos AES Encryption" on domain trusts, may be required to allow client communication across the trust relationship. false |

| | |
|---|---|
| Fix Text: | 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:<br><br>AES128_HMAC_SHA1<br>AES256_HMAC_SHA1<br>Future encryption types<br><br>Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting "The other domain supports Kerberos AES Encryption" on domain trusts, may be required to allow client communication across the trust relationship. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1214<br>Result: false<br>Title: Kerberos Encryption Types<br>Description: Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('Network Security: Configure encryption types allowed for Kerberos' is set to 'Enabled' with 'RC4_HMAC_MD5', 'AES128_HMAC_SHA1', 'AES256_HMAC_SHA1', 'Future encryption types') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:121400 (registry_test)<br>Result: false<br>Title: 'Network Security: Configure encryption types allowed for Kerberos' is set to 'Enabled' with 'RC4_HMAC_MD5', 'AES128_HMAC_SHA1', 'AES256_HMAC_SHA1', 'Future encryption types'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:121400 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters'<br>◦ name must be equal to 'SupportedEncryptionTypes'<br>State ID: oval:mil.disa.stig.windows:ste:121400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '2147483640'<br>Additional Information: Check existence requirement not met. |

## V-225056 - Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225056r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000400 |
| Identities: | CCE-44861-3<br>SV-88359<br>V-73695<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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). |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1219<br>Result: false<br>Title: Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.<br>Description: The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security')<br>▪ true ('Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require 128-bit encryption') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:459500 (registry_test)<br>Result: false<br>Title: 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:459500 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name must be equal to 'NTLMMinClientSec'<br>State ID: oval:mil.disa.fso.windows:ste:459500 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must match a 'bitwise and' comparison to '524288'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name equals 'NTLMMinClientSec'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '536870912'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.fso.windows:tst:459501 (registry_test)<br>Result: true<br>Title: 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require 128-bit encryption'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:459500 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name must be equal to 'NTLMMinClientSec'<br>State ID: oval:mil.disa.fso.windows:ste:459501 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must match a 'bitwise and' comparison to '536870912' |

## V-225057 - Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225057r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000410 |
| Identities: | CCE-46160-8<br>SV-88361<br>V-73697<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |
| Fix Text: | 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). |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1220<br>Result: false<br>Title: Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.<br>Description: The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false ('Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security')<br>▪ true ('Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require 128-bit encryption') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:459600 (registry_test)<br>Result: false<br>Title: 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:459600 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name must be equal to 'NTLMMinServerSec'<br><br>State ID: oval:mil.disa.fso.windows:ste:459500 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must match a 'bitwise and' comparison to '524288'<br>Collected Item/State Result:<br>[ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name equals 'NTLMMinServerSec'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '536870912'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.fso.windows:tst:459601 (registry_test)<br>Result: true<br>Title: 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require 128-bit encryption'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:459600 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'<br>◦ name must be equal to 'NTLMMinServerSec'<br>State ID: oval:mil.disa.fso.windows:ste:459501 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must match a 'bitwise and' comparison to '536870912' |

## V-225058 - Users must be required to enter a password to access private keys stored on the computer.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225058r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000420 |
| Identities: | CCE-46878-5<br>V-73699<br>SV-88363<br>CCI-000186 (NIST SP 800-53: IA-5 (2); NIST SP 800-53A: IA-5 (2).1; NIST SP 800-53 Rev 4: IA-5 (2) (b); NIST SP 800-53 Rev 5: IA-5 (2) (a) (1)) |
| Description: | 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.<br><br>The cornerstone of the PKI is the private key used to encrypt or digitally sign information.<br><br>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.<br><br>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. false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1221<br>Result: false<br>Title: Users must be required to enter a password to access private keys stored on the computer.<br>Description: Required to enter a password to access private keys<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (All child checks must be true.)<br>▪ false (HKEY_LOCAL_MACHINE\System\Policies\Microsoft\Cryptography\ForceKeyProtection exists and equals 2) |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.fso.windows:tst:497300 (registry_test)<br>Result: false<br>Title: HKEY_LOCAL_MACHINE\System\Policies\Microsoft\Cryptography\ForceKeyProtection exists and equals 2<br>Check Existence: All collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:497300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'SOFTWARE\Policies\Microsoft\Cryptography'<br>◦ name must be equal to 'ForceKeyProtection'<br><br>State ID: oval:mil.disa.fso.windows:ste:497300 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '2'<br>Additional Information: Check existence requirement not met. |

## V-225059 - Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225059r877398_rule |
| Result: | Fail |
| Version: | WN16-SO-000430 |
| Identities: | CCE-44610-4<br>V-73701<br>SV-88365<br>CCI-000068 (NIST SP 800-53: AC-17 (2); NIST SP 800-53A: AC-17 (2).1; NIST SP 800-53 Rev 4: AC-17 (2); NIST SP 800-53 Rev 5: AC-17 (2))<br>CCI-002450 (NIST SP 800-53 Rev 4: SC-13; NIST SP 800-53 Rev 5: SC-13 b) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000478-GPOS-00223 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1222<br>Result: false<br>Title: Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.<br>Description: The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Verifies 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:122200 (registry_test)<br>Result: false<br>Title: Verifies 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:460000 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy'<br>◦ name must be equal to 'Enabled'<br>State ID: oval:mil.disa.stig.windows:ste:122200 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: [ false ] ◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy'<br>◦ name equals 'Enabled'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '0'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

## V-225061 - User Account Control approval mode for the built-in Administrator must be enabled.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225061r852388_rule |
| Result: | Fail |
| Version: | WN16-SO-000460 |
| Identities: | CCE-47000-5<br>SV-88371<br>V-73707<br>CCI-002038 (NIST SP 800-53 Rev 4: IA-11) |

| | |
|---|---|
| Description: | 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.<br><br>Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1225<br>Result: false<br>Title: User Account Control approval mode for the built-in Administrator must be enabled.<br>Description: User Account Control approval mode for the built-in Administrator must be enabled.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Verifies 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:122500 (registry_test)<br>Result: false<br>Title: Verifies 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:460300 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name must be equal to 'FilterAdministratorToken'<br>State ID: oval:mil.disa.stig.windows:ste:122500 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-225063 - User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225063r569186_rule |
| Result: | Fail |
| Version: | WN16-SO-000480 |
| Identities: | CCE-47284-5<br>SV-88375<br>V-73711<br>CCI-001084 (NIST SP 800-53: SC-3; NIST SP 800-53A: SC-3.1 (ii); NIST SP 800-53 Rev 4: SC-3; NIST SP 800-53 Rev 5: SC-3) |
| Description: | 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. false |
| Fix Text: | 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".<br><br>The more secure option for this setting, "Prompt for credentials on the secure desktop", would also be acceptable. |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1227<br>Result: false<br>Title: User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.<br>Description: User Account Control must, at minimum, prompt administrators for consent.<br>Class: compliance<br>Tests: ◦ false (One or more child checks must be true.)<br>▪ false (Verifies 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent' or more secure options)<br>▪ false (Verifies 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is not set to 'Elevate without prompting') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:122700 (registry_test)<br>Result: false<br>Title: Verifies 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent' or more secure options<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:460400 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name must be equal to 'ConsentPromptBehaviorAdmin'<br>State ID: oval:mil.disa.stig.windows:ste:122700 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '2'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name equals 'ConsentPromptBehaviorAdmin'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '5'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value<br><br>Test ID: oval:mil.disa.stig.windows:tst:122701 (registry_test)<br>Result: false<br>Title: Verifies 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is not set to 'Elevate without prompting'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:460400 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name must be equal to 'ConsentPromptBehaviorAdmin'<br>State ID: oval:mil.disa.stig.windows:ste:122701 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '1'<br>Collected Item/State Result: [ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name equals 'ConsentPromptBehaviorAdmin'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '5'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

## V-225064 - User Account Control must automatically deny standard user requests for elevation.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225064r852389_rule |
| Result: | Fail |
| Version: | WN16-SO-000490 |
| Identities: | CCE-47214-2<br>SV-88377<br>V-73713<br>CCI-002038 (NIST SP 800-53 Rev 4: IA-11) |
| Description: | 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.<br><br>Satisfies: SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00156 false |
| Fix Text: | 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". |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1228<br>Result: false<br>Title: User Account Control must automatically deny standard user requests for elevation.<br>Description: User Account Control must automatically deny standard user requests for elevation.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (Verifies 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:122800 (registry_test)<br>Result: false<br>Title: Verifies 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.fso.windows:obj:460500 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name must be equal to 'ConsentPromptBehaviorUser'<br>State ID: oval:mil.disa.stig.windows:ste:122800 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ check_existence = 'at_least_one_exists', value must be equal to '0'<br>Collected Item/State Result:<br>[ false ]<br>◦ hive equals 'HKEY_LOCAL_MACHINE'<br>◦ key equals 'Software\Microsoft\Windows\CurrentVersion\Policies\System'<br>◦ name equals 'ConsentPromptBehaviorUser'<br>◦ last_write_time equals '133302937670000000'<br>◦ type equals 'reg_dword'<br>◦ value equals '3'<br>◦ windows_view equals '64_bit'<br>Additional Information: Check requirement not met.<br>value |

## V-225072 - The Allow log on locally user right must only be assigned to the Administrators group.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225072r569186_rule |
| Result: | Fail |
| Version: | WN16-UR-000050 |
| Identities: | CCE-45723-4<br>V-73739<br>SV-88403<br>CCI-000213 (NIST SP 800-53: AC-3; NIST SP 800-53A: AC-3.1; NIST SP 800-53 Rev 4: AC-3; NIST SP 800-53 Rev 5: AC-3) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>Accounts with the "Allow log on locally" user right can log on interactively to a system. false |
| Fix Text: | 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:<br><br>- Administrators |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1238<br>Result: false<br>Title: WN16-UR-000050<br>Description: The Allow log on locally user right must only be assigned to the Administrators group.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false (Allow log on locally - Administrators) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:123800 (accesstoken_test)<br>Result: false<br>Title: Allow log on locally - Administrators<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:123801 (accesstoken_object)<br>Object Requirements:<br>◦ Collect any available items.<br>Exclude Items If:<br>◦ security_principle equals 'Administrators'<br>State ID: oval:mil.disa.stig.windows:ste:123801 (accesstoken_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', seinteractivelogonright must be equal to '0'<br>Collected Item/State Result:<br>[ false ]<br>◦ seinteractivelogonright equals '1' for: Backup Operators, Users<br>◦ seinteractivelogonright equals '0' for Remote Management Users, Guests, NT SERVICE\ALL SERVICES, Power Users, Everyone, Performance Log Users, Administrator, DIALUP, PROXY, IUSR, LOCAL SERVICE, BATCH, SERVICE, DefaultAccount, Guest, ANONYMOUS LOGON, Storage Replica Administrators, CREATOR OWNER, Certificate Service DCOM Access, Performance Monitor Users, IIS_IUSRS, RDS Remote Access Servers, NETWORK SERVICE, Authenticated Users, Access Control Assistance Operators, System Managed Accounts Group, INTERACTIVE, CREATOR GROUP SERVER, TERMINAL SERVER USER, Cryptographic Operators, CREATOR GROUP, RDS Management Servers, Network Configuration Operators, RDS Endpoint Servers, Remote Desktop Users, Hyper-V Administrators, CREATOR OWNER SERVER, NT SERVICE\WdiServiceHost, Replicator, Distributed COM Users, Event Log Readers, Print Operators, ENTERPRISE DOMAIN CONTROLLERS, NETWORK, SYSTEM<br><br>Additional Information: Check requirement not met.<br>seinteractivelogonright<br>seinteractivelogonright |

## V-225073 - The Back up files and directories user right must only be assigned to the Administrators group.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225073r877392_rule |
| Result: | Fail |
| Version: | WN16-UR-000070 |
| Identities: | CCE-44987-6<br>SV-88407<br>V-73743<br>CCI-002235 (NIST SP 800-53 Rev 4: AC-6 (10); NIST SP 800-53 Rev 5: AC-6 (10)) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>Accounts with the "Back up files and directories" user right can circumvent file and directory permissions and could allow access to sensitive data. false |
| Fix Text: | 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:<br><br>- Administrators |
| Severity: | medium |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1239<br>Result: false<br>Title: WN16-UR-000070<br>Description: The Back up files and directories user right must only be assigned to the Administrators group.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Back up files and directories - Administrators) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:123900 (accesstoken_test)<br>Result: false<br>Title: Back up files and directories - Administrators<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:123900 (accesstoken_object)<br>Object Requirements: ◦ Collect any available items.<br>Exclude Items If: ◦ security_principle equals 'Administrators'<br>State ID: oval:mil.disa.stig.windows:ste:123900 (accesstoken_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', sebackupprivilege must be equal to '0'<br>Collected Item/State Result: ◦ sebackupprivilege equals '1' for: Backup Operators<br>[ false ] ◦ sebackupprivilege equals '0' for Remote Management Users, Guests, NT SERVICE\ALL SERVICES, Power Users, Everyone, Performance Log Users, Administrator, DIALUP, PROXY, IUSR, LOCAL SERVICE, BATCH, SERVICE, DefaultAccount, Guest, ANONYMOUS LOGON, Storage Replica Administrators, CREATOR OWNER, Certificate Service DCOM Access, Performance Monitor Users, IIS_IUSRS, RDS Remote Access Servers, NETWORK SERVICE, Authenticated Users, Access Control Assistance Operators, System Managed Accounts Group, INTERACTIVE, CREATOR GROUP SERVER, TERMINAL SERVER USER, Cryptographic Operators, CREATOR GROUP, RDS Management Servers, Network Configuration Operators, RDS Endpoint Servers, Remote Desktop Users, Hyper-V Administrators, CREATOR OWNER SERVER, NT SERVICE\WdiServiceHost, Replicator, Distributed COM Users, Event Log Readers, Print Operators, ENTERPRISE DOMAIN CONTROLLERS, Users, NETWORK, SYSTEM<br>Additional Information: Check requirement not met.<br>sebackupprivilege |

## V-225092 - The Restore files and directories user right must only be assigned to the Administrators group.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-225092r877392_rule |
| Result: | Fail |
| Version: | WN16-UR-000300 |
| Identities: | CCE-46176-4<br>SV-88465<br>V-73801<br>CCI-002235 (NIST SP 800-53 Rev 4: AC-6 (10); NIST SP 800-53 Rev 5: AC-6 (10)) |
| Description: | Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.<br><br>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. false |
| Fix Text: | 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:<br><br>- Administrators |
| Severity: | medium |
| Weight: | 10.0 |

| | |
|---|---|
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1256<br>Result: false<br>Title: WN16-UR-000300<br>Description: The Restore files and directories user right must only be assigned to the Administrators group.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false (Restore files and directories - Administrators) |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:125600 (accesstoken_test)<br>Result: false<br>Title: Restore files and directories - Administrators<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:125600 (accesstoken_object)<br>Object Requirements: ◦ Collect any available items.<br>Exclude Items If: ◦ security_principle equals 'Administrators'<br>State ID: oval:mil.disa.stig.windows:ste:125600 (accesstoken_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', serestoreprivilege must be equal to '0'<br>Collected Item/State Result: ◦ serestoreprivilege equals '1' for: Backup Operators<br>[ false ] ◦ serestoreprivilege equals '0' for Remote Management Users, Guests, NT SERVICE\ALL SERVICES, Power Users, Everyone, Performance Log Users, Administrator, DIALUP, PROXY, IUSR, LOCAL SERVICE, BATCH, SERVICE, DefaultAccount, Guest, ANONYMOUS LOGON, Storage Replica Administrators, CREATOR OWNER, Certificate Service DCOM Access, Performance Monitor Users, IIS_IUSRS, RDS Remote Access Servers, NETWORK SERVICE, Authenticated Users, Access Control Assistance Operators, System Managed Accounts Group, INTERACTIVE, CREATOR GROUP SERVER, TERMINAL SERVER USER, Cryptographic Operators, CREATOR GROUP, RDS Management Servers, Network Configuration Operators, RDS Endpoint Servers, Remote Desktop Users, Hyper-V Administrators, CREATOR OWNER SERVER, NT SERVICE\WdiServiceHost, Replicator, Distributed COM Users, Event Log Readers, Print Operators, ENTERPRISE DOMAIN CONTROLLERS, Users, NETWORK, SYSTEM<br>Additional Information: Check requirement not met.<br>serestoreprivilege |

# Detailed Results: Low Severity (CAT III)

### V-224916 - Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224916r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000040 |
| Identities: | CCE-45275-5<br>SV-88151<br>V-73499<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | Configuring the system to disable IPv6 source routing protects against spoofing. false |
| Fix Text: | 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.<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | low |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1084<br>Result: false<br>Title: IPv6 Source Routing<br>Description: Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Highest protection, source routing is completely disabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:108400 (registry_test)<br>Result: false<br><br>Title: 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Highest protection, source routing is completely disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:108400 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Services\Tcpip6\Parameters'<br>◦ name must be equal to 'DisableIPSourceRouting'<br>State ID: oval:mil.disa.stig.windows:ste:108400 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '2'<br>Additional Information: Check existence requirement not met. |

## V-224917 - Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224917r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000050 |
| Identities: | CCE-45276-3<br>SV-88153<br>V-73501<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | Configuring the system to disable IP source routing protects against spoofing. false |
| Fix Text: | 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.<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | low |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1085<br>Result: false<br>Title: Disable IP Source Routing<br>Description: Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Highest protection, source routing is completely disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:108500 (registry_test)<br>Result: false<br>Title: 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Highest protection, source routing is completely disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:108500 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Services\Tcpip\Parameters'<br>◦ name must be equal to 'DisableIPSourceRouting'<br>State ID: oval:mil.disa.stig.windows:ste:108500 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '2'<br>Additional Information: Check existence requirement not met. |

## V-224918 - Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224918r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000060 |
| Identities: | CCE-45279-7<br>SV-88155<br>V-73503<br>CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b) |
| Description: | 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. false |

| | |
|---|---|
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" to "Disabled".<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | low |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1086<br>Result: false<br>Title: Disable ICMP Redirect<br>Description: Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:108600 (registry_test)<br>Result: false<br>Title: 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:108600 (registry_object)<br>Object Requirements: ◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Services\Tcpip\Parameters'<br>◦ name must be equal to 'EnableICMPRedirect'<br>State ID: oval:mil.disa.stig.windows:ste:108600 (registry_state)<br>State Requirements: ◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '0'<br>Additional Information: Check existence requirement not met. |

## V-224919 - Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224919r852324_rule |
| Result: | Fail |
| Version: | WN16-CC-000070 |
| Identities: | CCE-45283-9<br>SV-88157<br>V-73505<br>CCI-002385 (NIST SP 800-53 Rev 4: SC-5; NIST SP 800-53 Rev 5: SC-5 a) |
| Description: | 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. false |
| Fix Text: | 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".<br><br>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 \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively. |
| Severity: | low |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1087<br>Result: false<br>Title: Name-Release Attacks<br>Description: Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.<br>Class: compliance<br>Tests: ◦ false (All child checks must be true.)<br>▪ false ('MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled') |

| | |
|---|---|
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:108700 (registry_test)<br>Result: false<br>Title: 'MSS: (NoNameReleaseOnDemand) Allow computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br><br>Object ID: oval:mil.disa.stig.windows:obj:108700 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'System\CurrentControlSet\Services\Netbt\Parameters'<br>◦ name must be equal to 'NoNameReleaseOnDemand'<br>State ID: oval:mil.disa.stig.windows:ste:108700 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |

## V-224931 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

| | |
|---|---|
| Rule ID: | xccdf_mil.disa.stig_rule_SV-224931r569186_rule |
| Result: | Fail |
| Version: | WN16-CC-000240 |
| Identities: | CCE-45945-3<br>V-73543<br>SV-88207<br>CCI-000381 (NIST SP 800-53: CM-7; NIST SP 800-53A: CM-7.1 (ii); NIST SP 800-53 Rev 4: CM-7 a; NIST SP 800-53 Rev 5: CM-7 a) |
| Description: | 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.<br><br>This setting will prevent the Program Inventory from collecting data about a system and sending the information to Microsoft. false |
| Fix Text: | Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Application Compatibility >> "Turn off Inventory Collector" to "Enabled". |
| Severity: | low |
| Weight: | 10.0 |
| Reference: | Title: DPMS Target Microsoft Windows Server 2016<br>Publisher: DISA<br>Type: DPMS Target<br>Subject: Microsoft Windows Server 2016<br>Identifier: 4205 |
| Definitions: | Definition ID: oval:mil.disa.stig.windows:def:1096<br>Result: false<br>Title: WN16-CC-000240<br>Description: The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.<br>Class: compliance<br>Tests:<br>◦ false (All child checks must be true.)<br>▪ false ('Turn off Inventory Collector' is set to 'Enabled') |
| Tests: | Test ID: oval:mil.disa.stig.windows:tst:109600 (registry_test)<br>Result: false<br>Title: 'Turn off Inventory Collector' is set to 'Enabled'<br>Check Existence: One or more collected items must exist.<br>Check: All collected items must match the given state(s).<br>Object ID: oval:mil.disa.stig.windows:obj:109600 (registry_object)<br>Object Requirements:<br>◦ hive must be equal to 'HKEY_LOCAL_MACHINE'<br>◦ key must be equal to 'Software\Policies\Microsoft\Windows\AppCompat'<br>◦ name must be equal to 'DisableInventory'<br>State ID: oval:mil.disa.stig.windows:ste:109600 (registry_state)<br>State Requirements:<br>◦ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword'<br>◦ for check = 'all', value, the following must be true:<br>▪ value must be equal to '1'<br>Additional Information: Check existence requirement not met. |