Tenable Vulnerability Management Report

Tenable Vulnerability Management

Tue, 16 Dec 2025 18:18:56 UTC

Table Of Contents

Vulnerabilities By Plugin....10

- 213824 (1) - Wireshark SEoL (2.2.x)....11
- 242325 (1) - SQLite < 3.50.2 Memory Corruption....12
- 56710 (1) - Wireshark / Ethereal Unsupported Version Detection....13
- 97574 (1) - Wireshark 2.0.x < 2.0.11 / 2.2.x < 2.2.5 Multiple DoS....14
- 101898 (1) - Wireshark 2.0.x < 2.0.14 / 2.2.x < 2.2.8 Multiple DoS....16
- 103569 (1) - Windows Defender Antimalware/Antivirus Signature Definition Check....18
- 250276 (1) - Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)....19
- 103985 (1) - Wireshark 2.2.x < 2.2.10 Multiple DoS....20
- 102920 (1) - Wireshark 2.2.x < 2.2.9 Multiple DoS....21
- 166555 (1) - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)....23
- 100671 (1) - Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS....25
- 99437 (1) - Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS....28
- 240237 (1) - SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities....31
- 111387 (1) - Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities....32
- 193266 (1) - Security Updates Outlook for Windows (April 2024)....34
- 81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)....35
- 157288 (1) - TLS Version 1.1 Deprecated Protocol....36
- 42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)....37
- 96765 (1) - Wireshark 2.0.x < 2.0.10 / 2.2.x < 2.2.4 Multiple DoS....38
- 107093 (1) - Wireshark 2.2.x < 2.2.13 / 2.4.x < 2.4.5 Multiple DoS Vulnerabilities....39
- 108885 (1) - Wireshark 2.2.x < 2.2.14 / 2.4.x < 2.4.6 Multiple Vulnerabilities....41
- 117339 (1) - Wireshark 2.2.x < 2.2.17 / 2.4.x < 2.4.9 / 2.6.x < 2.6.3 Multiple Vulnerabilities....43
- 106142 (1) - Wireshark 2.2.x < 2.2.12 / 2.4.x < 2.4.4 DoS Vulnerabilities....44
- 110269 (1) - Wireshark 2.2.x < 2.2.15 / 2.4.x < 2.4.7 / 2.6.x < 2.6.1 Multiple Vulnerabilities....45
- 51192 (1) - SSL Certificate Cannot Be Trusted....47
- 95435 (1) - Wireshark 2.0.x < 2.0.8 / 2.2.x < 2.2.2 Multiple DoS....48
- 57582 (1) - SSL Self-Signed Certificate....50
- 176372 (1) - Wireshark 2.2.x < 2.2.17 Multiple Vulnerabilities....51
- 104743 (1) - TLS Version 1.0 Protocol Detection....53
- 26928 (1) - SSL Weak Cipher Suites Supported....54
- 65821 (1) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)....56
- 105007 (1) - Wireshark 2.2.x < 2.2.11 / 2.4.x < 2.4.3 DoS Vulnerabilities....58
- 264898 (1) - Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)....59
- 10114 (1) - ICMP Timestamp Request Remote Date Disclosure....60

Assets Summary (Executive)....61

- lognpacific3286....62

Remediations....64

- Suggested Remediations....65

Audits FAILED....66

- WN11-00-000031 - Windows 11 systems must use a BitLocker PIN for pre-boot authentication....67
- WN11-00-000032 - Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication....69
- WN11-00-000090 - Accounts must be configured to require password expiration....71

- WN11-00-000125 - Copilot in Windows must be disabled for Windows 11 73
- WN11-00-000135 - A host-based firewall must be installed and enabled on the system 75
- WN11-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut 77
- WN11-00-000150 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled 78
- WN11-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system 79
- WN11-00-000175 - The Secondary Logon service must be disabled on Windows 11 81
- WN11-00-000260 - The Windows 11 time service must synchronize with an appropriate DOD time source 83
- WN11-AC-000005 - Windows 11 account lockout duration must be configured to 15 minutes or greater 85
- WN11-AC-000010 - The number of allowed bad logon attempts must be configured to three or less 87
- WN11-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes 89
- WN11-AC-000020 - The password history must be configured to 24 passwords remembered 91
- WN11-AC-000030 - The minimum password age must be configured to at least 1 day 93
- WN11-AC-000035 - Passwords must, at a minimum, be 14 characters 95
- WN11-AC-000040 - The built-in Microsoft password complexity filter must be enabled 97
- WN11-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures 99
- WN11-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes 101
- WN11-AU-000035 - The system must be configured to audit Account Management - User Account Management failures 103
- WN11-AU-000045 - The system must be configured to audit Detailed Tracking - PNP Activity successes 104
- WN11-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes 107
- WN11-AU-000054 - The system must be configured to audit Logon/Logoff - Account Lockout failures 110
- WN11-AU-000060 - The system must be configured to audit Logon/Logoff - Group Membership successes 112
- WN11-AU-000081 - Windows 11 must be configured to audit Object Access - File Share failures 114
- WN11-AU-000082 - Windows 11 must be configured to audit Object Access - File Share successes 116
- WN11-AU-000083 - Windows 11 must be configured to audit Object Access - Other Object Access Events successes 118
- WN11-AU-000084 - Windows 11 must be configured to audit Object Access - Other Object Access Events failures 120
- WN11-AU-000085 - The system must be configured to audit Object Access - Removable Storage failures 122
- WN11-AU-000090 - The system must be configured to audit Object Access - Removable Storage successes 124
- WN11-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes 126
- WN11-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures 128
- WN11-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes 130
- WN11-AU-000120 - The system must be configured to audit System - IPsec Driver failures 132
- WN11-AU-000150 - The system must be configured to audit System - Security System Extension successes 134
- WN11-AU-000500 - The Application event log size must be configured to 32768 KB or greater 136
- WN11-AU-000505 - The Security event log size must be configured to 1024000 KB or greater 137
- WN11-AU-000510 - The System event log size must be configured to 32768 KB or greater 138
- WN11-AU-000550 - Windows 11 must be configured to audit Other Policy Change Events Successes 139
- WN11-AU-000555 - Windows 11 must be configured to audit Other Policy Change Events Failures 141
- WN11-AU-000560 - Windows 11 must be configured to audit other Logon/Logoff Events Successes 143
- WN11-AU-000565 - Windows 11 must be configured to audit other Logon/Logoff Events Failures 145
- WN11-AU-000570 - Windows 11 must be configured to audit Detailed File Share Failures 147
- WN11-AU-000575 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Successes 149

- WN11-AU-000580 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Failures..... 151
- WN11-AU-000585 - Windows 11 must have command line process auditing events enabled for failures..... 153
- WN11-CC-000005 - Camera access from the lock screen must be disabled..... 155
- WN11-CC-000007 - Windows 11 must cover or disable the built-in or attached camera when not in use..... 157
- WN11-CC-000010 - The display of slide shows on the lock screen must be disabled..... 159
- WN11-CC-000020 - IPv6 source routing must be configured to highest protection..... 161
- WN11-CC-000025 - The system must be configured to prevent IP source routing.....162
- WN11-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes..... 163
- WN11-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers..... 164
- WN11-CC-000038 - WDigest Authentication must be disabled..... 166
- WN11-CC-000039 - Run as different user must be removed from context menus..... 168
- WN11-CC-000040 - Insecure logons to an SMB server must be disabled..... 170
- WN11-CC-000044 - Internet connection sharing must be disabled..... 171
- WN11-CC-000050 - Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.....173
- WN11-CC-000052 - Windows 11 must be configured to prioritize ECC Curves with longer key lengths first.....175
- WN11-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.....176
- WN11-CC-000065 - Wi-Fi Sense must be disabled.....177
- WN11-CC-000066 - Command line data must be included in process creation events.....178
- WN11-CC-000068 - Windows 11 must be configured to enable Remote host allows delegation of non-exportable credentials.....180
- WN11-CC-000070 - Virtualization-based Security must be enabled on Windows 11 with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.....181
- WN11-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers..... 183
- WN11-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.....185
- WN11-CC-000100 - Downloading print driver packages over HTTP must be prevented.....186
- WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers..... 188
- WN11-CC-000110 - Printing over HTTP must be prevented..... 190
- WN11-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.....192
- WN11-CC-000145 - Users must be prompted for a password on resume from sleep (on battery)..... 194
- WN11-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in)..... 195
- WN11-CC-000155 - Solicited Remote Assistance must not be allowed..... 196
- WN11-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server..... 197
- WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled..... 198
- WN11-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.....199
- WN11-CC-000180 - Autoplay must be turned off for non-volume devices.....201
- WN11-CC-000185 - The default autorun behavior must be configured to prevent autorun commands..... 202
- WN11-CC-000190 - Autoplay must be disabled for all drives.....203
- WN11-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.....204
- WN11-CC-000197 - Microsoft consumer experiences must be turned off..... 205
- WN11-CC-000200 - Administrator accounts must not be enumerated during elevation..... 207
- WN11-CC-000204 - Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.....208

- WN11-CC-000205 - Windows Telemetry must not be configured to Full..... 209
- WN11-CC-000206 - Windows Update must not obtain updates from other PCs on the internet..... 210
- WN11-CC-000210 - The Microsoft Defender SmartScreen for Explorer must be enabled..... 211
- WN11-CC-000252 - Windows 11 must be configured to disable Windows Game Recording and Broadcasting.... 213
- WN11-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled..... 215
- WN11-CC-000260 - Windows 11 must be configured to require a minimum pin length of six characters or greater..... 216
- WN11-CC-000270 - Passwords must not be saved in the Remote Desktop Client..... 217
- WN11-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts..... 218
- WN11-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection..... 219
- WN11-CC-000285 - The Remote Desktop Session Host must require secure RPC communications..... 220
- WN11-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level..... 222
- WN11-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds..... 224
- WN11-CC-000305 - Indexing of encrypted files must be turned off..... 225
- WN11-CC-000310 - Users must be prevented from changing installation options..... 227
- WN11-CC-000315 - The Windows Installer feature 'Always install with elevated privileges' must be disabled..... 228
- WN11-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled..... 229
- WN11-CC-000326 - PowerShell script block logging must be enabled on Windows 11..... 230
- WN11-CC-000327 - PowerShell Transcription must be enabled on Windows 11..... 232
- WN11-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication..... 234
- WN11-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic..... 235
- WN11-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication.... 236
- WN11-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic..... 237
- WN11-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials..... 238
- WN11-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication..... 239
- WN11-CC-000365 - Windows 11 must be configured to prevent Windows apps from being activated by voice while the system is locked..... 240
- WN11-CC-000370 - The convenience PIN for Windows 11 must be disabled..... 242
- WN11-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock..... 244
- WN11-CC-000390 - Windows 11 must be configured to prevent users from receiving suggestions for third-party or additional applications..... 245
- WN11-CC-000391 - Internet Explorer must be disabled for Windows 11..... 247
- WN11-EP-000310 - Windows 11 Kernel (Direct Memory Access) DMA Protection must be enabled..... 248
- WN11-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store..... 250
- WN11-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems..... 252
- WN11-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems..... 254
- WN11-PK-000020 - The US DOD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems..... 255
- WN11-SO-000005 - The built-in administrator account must be disabled..... 257
- WN11-SO-000010 - The built-in guest account must be disabled..... 259
- WN11-SO-000025 - The built-in guest account must be renamed..... 261
- WN11-SO-000030 - Audit policy using subcategories must be enabled..... 262
- WN11-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver..... 264
- WN11-SO-000075 - The required legal notice must be configured to display before console logon..... 266

- WN11-SO-000080 - The Windows message title for the legal notice must be configured..... 268
- WN11-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.... 270
- WN11-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing..... 271
- WN11-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.....273
- WN11-SO-000150 - Anonymous enumeration of shares must be restricted.....275
- WN11-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators..... 276
- WN11-SO-000180 - NTLM must be prevented from falling back to a Null session.....278
- WN11-SO-000185 - PKU2U authentication using online identities must be prevented.....279
- WN11-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.....280
- WN11-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM..... 281
- WN11-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients..... 282
- WN11-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers..... 283
- WN11-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.....284
- WN11-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled..... 286
- WN11-SO-000250 - User Account Control must prompt administrators for consent on the secure desktop..... 287
- WN11-SO-000255 - User Account Control must automatically deny elevation requests for standard users..... 288
- WN11-SO-000280 - Passwords for enabled local Administrator accounts must be changed at least every 60 days..... 289
- WN11-UC-000015 - Toast notifications to the lock screen must be turned off..... 291
- WN11-UR-000010 - The 'Access this computer from the network' user right must only be assigned to the Administrators and Remote Desktop Users groups..... 293
- WN11-UR-000025 - The 'Allow log on locally' user right must only be assigned to the Administrators and Users groups.....295
- WN11-UR-000030 - The 'Back up files and directories' user right must only be assigned to the Administrators group.....297
- WN11-UR-000070 - The 'Deny access to this computer from the network' user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems..... 299
- WN11-UR-000085 - The 'Deny log on locally' user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.....301
- WN11-UR-000090 - The 'Deny log on through Remote Desktop Services' user right on Windows 11 workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.....303
- WN11-UR-000110 - The 'Impersonate a client after authentication' user right must only be assigned to Administrators, Service, Local Service, and Network Service.....306
- WN11-UR-000160 - The 'Restore files and directories' user right must only be assigned to the Administrators group.....308

Audits SKIPPED..... 310

Audits PASSED..... 311

- DISA_Microsoft_Windows_11_STIG_v2r4.audit from DISA Microsoft Windows 11 STIG v2r4.....312
- WN11-00-000005 - Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version..... 313
- WN11-00-000010 - Windows 11 domain-joined systems must have a Trusted Platform Module (TPM) enabled..... 314
- WN11-00-000015 - Windows 11 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.....316
- WN11-00-000020 - Secure Boot must be enabled on Windows 11 systems.....318

- WN11-00-000040 - Windows 11 systems must be maintained at a supported servicing level..... 320
- WN11-00-000045 - The Windows 11 system must use an antivirus program..... 321
- WN11-00-000050 - Local volumes must be formatted using NTFS..... 323
- WN11-00-000075 - Only accounts responsible for the backup operations must be members of the Backup Operators group..... 325
- WN11-00-000080 - Only authorized user accounts must be allowed to create or run virtual machines on Windows 11 systems..... 327
- WN11-00-000085 - Standard local user accounts must not exist on a system in a domain..... 329
- WN11-00-000095 - Permissions for system files and directories must conform to minimum requirements..... 330
- WN11-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation..... 332
- WN11-00-000105 - Simple Network Management Protocol (SNMP) must not be installed on the system..... 334
- WN11-00-000110 - Simple TCP/IP Services must not be installed on the system..... 336
- WN11-00-000115 - The Telnet Client must not be installed on the system..... 338
- WN11-00-000120 - The TFTP Client must not be installed on the system..... 340
- WN11-00-000160 - The Server Message Block (SMB) v1 protocol must be disabled on the system..... 342
- WN11-00-000165 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server..... 344
- WN11-00-000170 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client..... 346
- WN11-00-000210 - Bluetooth must be turned off unless approved by the organization..... 348
- WN11-00-000220 - Bluetooth must be turned off when not in use..... 350
- WN11-00-000395 - Windows 11 must not have portproxy enabled or in use..... 352
- WN11-AC-000025 - The maximum password age must be configured to 60 days or less..... 354
- WN11-AC-000045 - Reversible password encryption must be disabled..... 356
- WN11-AU-000030 - The system must be configured to audit Account Management - Security Group Management successes..... 358
- WN11-AU-000040 - The system must be configured to audit Account Management - User Account Management successes..... 360
- WN11-AU-000065 - The system must be configured to audit Logon/Logoff - Logoff successes..... 362
- WN11-AU-000070 - The system must be configured to audit Logon/Logoff - Logon failures..... 364
- WN11-AU-000075 - The system must be configured to audit Logon/Logoff - Logon successes..... 366
- WN11-AU-000080 - The system must be configured to audit Logon/Logoff - Special Logon successes..... 368
- WN11-AU-000100 - The system must be configured to audit Policy Change - Audit Policy Change successes.... 370
- WN11-AU-000105 - The system must be configured to audit Policy Change - Authentication Policy Change successes..... 372
- WN11-AU-000130 - The system must be configured to audit System - Other System Events successes..... 374
- WN11-AU-000135 - The system must be configured to audit System - Other System Events failures..... 376
- WN11-AU-000140 - The system must be configured to audit System - Security State Change successes..... 378
- WN11-AU-000155 - The system must be configured to audit System - System Integrity failures..... 380
- WN11-AU-000160 - The system must be configured to audit System - System Integrity successes..... 382
- WN11-AU-000515 - Windows 11 permissions for the Application event log must prevent access by non-privileged accounts..... 384
- WN11-AU-000520 - Windows 11 permissions for the Security event log must prevent access by non-privileged accounts..... 386
- WN11-AU-000525 - Windows 11 permissions for the System event log must prevent access by non-privileged accounts..... 388
- WN11-CC-000037 - Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems..... 390
- WN11-CC-000055 - Simultaneous connections to the internet or a Windows domain must be limited..... 391
- WN11-CC-000063 - Windows 11 systems must use either Group Policy or an approved Mobile Device Management (MDM) product to enforce STIG compliance..... 393

- WN11-CC-000075 - Credential Guard must be running on Windows 11 domain-joined systems..... 394
- WN11-CC-000080 - Virtualization-based protection of code integrity must be enabled..... 396
- WN11-CC-000115 - Systems must at least attempt device authentication using certificates..... 398
- WN11-CC-000130 - Local users on domain-joined computers must not be enumerated..... 399
- WN11-CC-000215 - Explorer Data Execution Prevention must be enabled..... 401
- WN11-CC-000220 - File Explorer heap termination on corruption must be disabled..... 402
- WN11-CC-000225 - File Explorer shell protocol must run in protected mode..... 403
- WN11-CC-000300 - Basic authentication for RSS feeds over HTTP must not be used..... 404
- WN11-CC-000320 - Users must be notified if a web-based program attempts to install software..... 406
- WN11-RG-000005 - Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained..... 407
- WN11-SO-000015 - Local accounts with blank passwords must be restricted to prevent access from the network..... 410
- WN11-SO-000020 - The built-in administrator account must be renamed..... 411
- WN11-SO-000035 - Outgoing secure channel traffic must be encrypted or signed..... 412
- WN11-SO-000040 - Outgoing secure channel traffic must be encrypted..... 415
- WN11-SO-000045 - Outgoing secure channel traffic must be signed..... 418
- WN11-SO-000050 - The computer account password must not be prevented from being reset..... 421
- WN11-SO-000055 - The maximum age for machine account passwords must be configured to 30 days or less..... 422
- WN11-SO-000060 - The system must be configured to require a strong session key..... 423
- WN11-SO-000085 - Caching of logon credentials must be limited..... 425
- WN11-SO-000110 - Unencrypted passwords must not be sent to third-party SMB Servers..... 426
- WN11-SO-000140 - Anonymous SID/Name translation must not be allowed..... 428
- WN11-SO-000145 - Anonymous enumeration of SAM accounts must not be allowed..... 429
- WN11-SO-000160 - The system must be configured to prevent anonymous users from having the same rights as the Everyone group..... 430
- WN11-SO-000165 - Anonymous access to Named Pipes and Shares must be restricted..... 431
- WN11-SO-000195 - The system must be configured to prevent the storage of the LAN Manager hash of passwords..... 432
- WN11-SO-000210 - The system must be configured to the required LDAP client signing level..... 434
- WN11-SO-000240 - The default permissions of global system objects must be increased..... 435
- WN11-SO-000251 - Windows 11 must use multifactor authentication for local and network access to privileged and nonprivileged accounts..... 436
- WN11-SO-000260 - User Account Control must be configured to detect application installations and prompt for elevation..... 438
- WN11-SO-000265 - User Account Control must only elevate UIAccess applications that are installed in secure locations..... 439
- WN11-SO-000270 - User Account Control must run all administrators in Admin Approval Mode, enabling UAC..... 440
- WN11-SO-000275 - User Account Control must virtualize file and registry write failures to per-user locations..... 441
- WN11-UC-000020 - Zone information must be preserved when saving attachments..... 442
- WN11-UR-000005 - The 'Access Credential Manager as a trusted caller' user right must not be assigned to any groups or accounts..... 443
- WN11-UR-000015 - The 'Act as part of the operating system' user right must not be assigned to any groups or accounts..... 445
- WN11-UR-000035 - The 'Change the system time' user right must only be assigned to Administrators and Local Service..... 447
- WN11-UR-000040 - The 'Create a pagefile' user right must only be assigned to the Administrators group..... 449
- WN11-UR-000045 - The 'Create a token object' user right must not be assigned to any groups or accounts..... 451

- WN11-UR-000050 - The 'Create global objects' user right must only be assigned to Administrators, Service, Local Service, and Network Service....453
- WN11-UR-000055 - The 'Create permanent shared objects' user right must not be assigned to any groups or accounts....455
- WN11-UR-000060 - The 'Create symbolic links' user right must only be assigned to the Administrators group.....457
- WN11-UR-000065 - The 'Debug programs' user right must only be assigned to the Administrators group.....459
- WN11-UR-000075 - The 'Deny log on as a batch job' user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts....461
- WN11-UR-000080 - The 'Deny log on as a service' user right on Windows 11 domain-joined workstations must be configured to prevent access from highly privileged domain accounts....463
- WN11-UR-000095 - The 'Enable computer and user accounts to be trusted for delegation' user right must not be assigned to any groups or accounts....465
- WN11-UR-000100 - The 'Force shutdown from a remote system' user right must only be assigned to the Administrators group....467
- WN11-UR-000120 - The 'Load and unload device drivers' user right must only be assigned to the Administrators group....469
- WN11-UR-000125 - The 'Lock pages in memory' user right must not be assigned to any groups or accounts.....471
- WN11-UR-000130 - The 'Manage auditing and security log' user right must only be assigned to the Administrators group....473
- WN11-UR-000140 - The 'Modify firmware environment values' user right must only be assigned to the Administrators group....475
- WN11-UR-000145 - The 'Perform volume maintenance tasks' user right must only be assigned to the Administrators group....477
- WN11-UR-000150 - The 'Profile single process' user right must only be assigned to the Administrators group....479
- WN11-UR-000165 - The 'Take ownership of files or other objects' user right must only be assigned to the Administrators group....481

Audits INFO,WARNING,ERROR....483

- WN11-00-000025 - Windows 11 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: Continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP)....484
- WN11-00-000030 - Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest....486
- WN11-00-000035 - The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs....488
- WN11-00-000055 - Alternate operating systems must not be permitted on the same system....490
- WN11-00-000060 - Non-system-created file shares on a system must limit access to groups that require it.....491
- WN11-00-000065 - Unused accounts must be disabled or removed from the system after 35 days of inactivity....492
- WN11-00-000070 - Only accounts responsible for the administration of a system must have Administrator rights on the system....495
- WN11-00-000130 - Software certificate installation files must be removed from Windows 11....497
- WN11-00-000140 - Inbound exceptions to the firewall on Windows 11 domain workstations must only allow authorized remote management hosts....498
- WN11-00-000190 - Orphaned security identifiers (SIDs) must be removed from user rights on Windows 11....501
- WN11-00-000230 - The system must notify the user when a Bluetooth device attempts to connect....502
- WN11-00-000240 - Administrative accounts must not be used with applications that access the internet, such as web browsers, or with potential internet sources, such as email....503
- WN11-00-000250 - Windows 11 nonpersistent VM sessions must not exceed 24 hours....505

Vulnerabilities By Plugin

213824 (1) - Wireshark SEoL (2.2.x)

Synopsis

An unsupported version of Wireshark is installed on the remote host.

Description

According to its version, Wireshark is 2.2.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

https://wiki.wireshark.org/Development/LifeCycle

Solution

Upgrade to a version of Wireshark that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2025/01/10, Modification date: 2025/01/10

Assets

lognpacific3286 (TCP/0) Vulnerability State: Active

```
Path                                : C:\Program Files\Wireshark
Installed version                   : 2.2.1
Security End of Life                : September 6, 2018
Time since Security End of Life (Est.) : >= 7 years
```

242325 (1) - SQLite < 3.50.2 Memory Corruption

Synopsis

The remote host is missing multiple security updates.

Description

The version of SQLite installed on the remote host is prior to 3.50.2. It is, therefore, affected by a memory corruption issue. The vulnerability can occur where the number of aggregate terms could exceed the number of columns available, leading to memory corruption.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.sqlite.org/cves.html

Solution

Upgrade to SQLite 3.50.2 or later.

Risk Factor

Critical

Vulnerability Priority Rating (VPR)

9.0

CVSS v3.0 Base Score

9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

CVE	CVE-2025-6965
XREF	IAVA-2025-A-0529

Plugin Information:

Publication date: 2025/07/18, Modification date: 2025/09/26

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe\sqlite3.dll
Installed version : 3.46.1.0
Fixed version     : 3.50.2


Path              : C:\Windows\System32\winsqlite3.dll
Installed version : 3.43.2.0
Fixed version     : 3.50.2


Path              : C:\Windows\SysWOW64\winsqlite3.dll
Installed version : 3.43.2.0
Fixed version     : 3.50.2
```

56710 (1) - Wireshark / Ethereal Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of Wireshark / Ethereal.

Description

According to its version, the installation of Wireshark / Ethereal on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://wiki.wireshark.org/Development/LifeCycle

Solution

Upgrade to a version of Wireshark that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA-0001-A-0624

Plugin Information:

Publication date: 2011/11/04, Modification date: 2021/06/10

Assets

lognpacific3286 (TCP/0) Vulnerability State: Active

```
Path                : C:\Program Files\Wireshark
Installed version   : 2.2.1
End of support date : September 7, 2018
Supported versions  : 3.2.x, 3.4.x
```

97574 (1) - Wireshark 2.0.x < 2.0.11 / 2.2.x < 2.2.5 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.11 or 2.2.x prior to 2.2.5. It is, therefore, affected by multiple denial of service vulnerabilities :
- An infinite loop condition exists in the Netscaler file parser in the nstrace_read_v20() and nstrace_read_v30() functions within file wiretap/netscaler.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this, via a specially crafted capture file, to consume excessive memory resources, resulting in a denial of service condition. (CVE-2017-6467)
- An out-of-bounds read error exists within various functions in file wiretap/netscaler.c when handling record lengths. An unauthenticated, remote attacker can exploit this, via a specially crafted capture file, to crash the Netscaler file parser process. (CVE-2017-6468)
- A memory allocation issue exists in the dissect_ldss_transfer() function within file epan/dissectors/packet-ldss.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this, via packet injection or a specially crafted capture file, to crash the LDSS dissector process. (CVE-2017-6469)
- An infinite loop condition exists in IAX2 in the iax2_add_ts_fields() function within file epan/dissectors/packet-iax2.c when processing timestamps. An unauthenticated, remote attacker can exploit this, via packet injection or a specially crafted capture file, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2017-6470)
- An infinite loop condition exists in WSP in the dissect_wsp_common() function within file epan/dissectors/packet-wsp.c when handling capability lengths. An unauthenticated, remote attacker can exploit this, via packet injection or a specially crafted capture file, to cause a denial of service condition. (CVE-2017-6471)
- An infinite loop condition exists in the RTMPT dissector in the dissect_rtmpt_common() function within file epan/dissectors/packet-rtmpt.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this, via packet injection or a specially crafted capture file, to consume excessive memory resources, resulting in a denial of service condition. (CVE-2017-6472)
- A denial of service vulnerability exists in the process_packet_data() function within file wiretap/k12.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this, via a specially crafted capture file, to crash the K12 file parser process. (CVE-2017-6473)
- An infinite loop condition exists in the NetScaler file parser in the nstrace_read_v10(), nstrace_read_v20(), and nstrace_read_v30() functions within file wiretap/netscaler.c when handling record sizes. An unauthenticated, remote attacker can exploit this, via a specially crafted capture file, to consume excessive memory resources, resulting in a denial of service condition. (CVE-2017-6474)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/security/wnpa-sec-2017-03.html

https://www.wireshark.org/security/wnpa-sec-2017-04.html

https://www.wireshark.org/security/wnpa-sec-2017-05.html

https://www.wireshark.org/security/wnpa-sec-2017-07.html

https://www.wireshark.org/security/wnpa-sec-2017-08.html

https://www.wireshark.org/security/wnpa-sec-2017-09.html

https://www.wireshark.org/security/wnpa-sec-2017-10.html

https://www.wireshark.org/security/wnpa-sec-2017-11.html

Solution

Upgrade to Wireshark version 2.0.11 / 2.2.5 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-6474
CVE	CVE-2017-6473
CVE	CVE-2017-6472
CVE	CVE-2017-6471
CVE	CVE-2017-6470
CVE	CVE-2017-6469
CVE	CVE-2017-6468
CVE	CVE-2017-6467

Plugin Information:

Publication date: 2017/03/07, Modification date: 2023/03/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.5
```

101898 (1) - Wireshark 2.0.x < 2.0.14 / 2.2.x < 2.2.8 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.14 or 2.2.x prior to 2.2.8. It is, therefore, affected by multiple denial of service vulnerabilities :
- A denial of service vulnerability exists in the DAAP dissector, specifically in the dissect_daap_one_tag() function within file epan/dissectors/packet-daap.c. An unauthenticated, remote attacker can exploit this to exhaust stack resources through uncontrolled recursion.
(CVE-2017-9617)
- An infinite loop condition exists in the DOCSIS dissector, specifically in the dissect_docsis() function within file plugins/docsis/packet-docsis.c. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace, to consume available CPU resources, resulting in a denial of service condition. (CVE-2017-11406)
- A memory allocation issue exists in the MQ dissector, specifically in the reassemble_mq() function within file epan/dissectors/packet-mq.c, due to improper validation of fragment lengths before attempting reassembly. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace, to cause a denial of service condition. (CVE-2017-11407)
- A flaw exists in the AMQP dissector, specifically in the get_amqp_1_0_value_formatter() function within file epan/dissectors/packet-amqp.c, when decoding lists.
An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace, to cause a stack overflow, resulting in a denial of service condition. (CVE-2017-11408)
- A large loop condition exists in the GPRS LLC dissector, specifically in the llc_gprs_dissect_xid() function within file epan/dissectors/packet-gprs-llc.c, when handling specially crafted packet or trace files. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this issue only applies to version 2.0.x.
(CVE-2017-11409)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/docs/relnotes/wireshark-2.0.14.html

https://www.wireshark.org/docs/relnotes/wireshark-2.2.8.html

https://www.wireshark.org/security/wnpa-sec-2017-34.html

https://www.wireshark.org/security/wnpa-sec-2017-35.html

https://www.wireshark.org/security/wnpa-sec-2017-36.html

https://www.wireshark.org/security/wnpa-sec-2017-37.html

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13799

Solution

Upgrade to Wireshark version 2.0.14 / 2.2.8 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-9617
CVE	CVE-2017-11409
CVE	CVE-2017-11408
CVE	CVE-2017-11407
CVE	CVE-2017-11406
BID	99087

Plugin Information:

Publication date: 2017/07/21, Modification date: 2025/12/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.8
```

103569 (1) - Windows Defender Antimalware/Antivirus Signature Definition Check

Synopsis

Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old

Description

Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day.

See Also

https://www.microsoft.com/en-us/wdsi/definitions

Solution

Trigger an update manually and/or enable auto-updates.

Risk Factor

High

Plugin Information:

Publication date: 2017/10/02, Modification date: 2024/08/06

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Malware Signature Timestamp : Sep. 17, 2025 at 02:08:41 GMT
Malware Signature Version   : 1.437.1.0
```

250276 (1) - Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)

Synopsis

Microsoft Teams for Desktop is affected by a remote code execution vulnerability.

Description

The version of Microsoft Teams for Desktop on the remote Windows host is prior to 25122.1415.3698.6812 It is, therefore, affected by a remote code execution vulnerability:
- Heap-based buffer overflow in Microsoft Teams allows an unauthorized attacker to execute code over a network. (CVE-2025-53783)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?8c9e5451

Solution

Upgrade to Microsoft Teams for Desktop version 25122.1415.3698.6812 or later via the Microsoft Store.

Risk Factor

High

Vulnerability Priority Rating (VPR)

6.7

CVSS v3.0 Base Score

7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS Base Score

7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

CVE	CVE-2025-53783
XREF	IAVA-2025-A-0600

Plugin Information:

Publication date: 2025/08/15, Modification date: 2025/08/15

Assets

lognpacific3286 (TCP/0) Vulnerability State: Active

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 25122.1415.3698.6812
```

103985 (1) - Wireshark 2.2.x < 2.2.10 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.10. It is, therefore, affected by multiple denial of service vulnerabilities in the DMP, BT ATT and MBIM dissectors. An unauthenticated, remote attacker can exploit this by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/security/wnpa-sec-2017-42.html

https://www.wireshark.org/security/wnpa-sec-2017-43.html

https://www.wireshark.org/security/wnpa-sec-2017-44.html

Solution

Upgrade to Wireshark version 2.2.10 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-15193
CVE	CVE-2017-15192
CVE	CVE-2017-15191
BID	101240
BID	101235
BID	101227

Plugin Information:

Publication date: 2017/10/19, Modification date: 2025/11/18

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.10
```

102920 (1) - Wireshark 2.2.x < 2.2.9 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.9. It is, therefore, affected by multiple denial of service vulnerabilities in the IrCOMM, Profinet I/O, and MSDP dissectors. An unauthenticated, remote attacker can exploit this by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/docs/relnotes/wireshark-2.2.9.html

https://www.wireshark.org/security/wnpa-sec-2017-38.html

https://www.wireshark.org/security/wnpa-sec-2017-39.html

https://www.wireshark.org/security/wnpa-sec-2017-41.html

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13847

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13929

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13933

Solution

Upgrade to Wireshark version 2.2.9 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-13767
CVE	CVE-2017-13766
CVE	CVE-2017-13765

Plugin Information:

Publication date: 2017/09/01, Modification date: 2025/11/24

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
```

```
Fixed version     : 2.2.9
```

166555 (1) - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Synopsis

The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

http://www.nessus.org/u?9780b9d2

Solution

Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
\EnableCertPaddingCheck

Risk Factor

High

Vulnerability Priority Rating (VPR)

9.0

CVSS v3.0 Base Score

8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.4 (E:H/RL:O/RC:C)

CVSS Base Score

7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.6 (E:H/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2013-3900
XREF	CISA-KNOWN-EXPLOITED-2022/07/10
XREF	IAVA-2013-A-0227

Plugin Information:

Publication date: 2022/10/26, Modification date: 2025/10/22

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Nessus detected the following potentially insecure registry key configuration:
   - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the
registry.
   - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not
present in the registry.
```

100671 (1) - Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.13 or 2.2.x prior to 2.2.7. It is, therefore, affected by multiple denial of service vulnerabilities :
- A NULL pointer dereference flaw exists in the dissect_msnip() function within file epan/dissectors/packet-msnip.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. (CVE-2017-9343)
- A divide-by-zero error exists in the dissect_connparamrequest() function within file epan/dissectors/packet-btl2cap.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. (CVE-2017-9344)
- An infinite loop condition exists in the expand_dns_name() function within file epan/dissectors/packet-dns.c when handling packets or packet trace files. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2017-9345)
- An infinite loop condition exists in the dissect_slsk_pdu() function within file epan/dissectors/packet-slsk.c when handling packets or packet trace files. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2017-9346)
- A NULL pointer dereference flaw exists in the ros_try_string() function within file epan/dissectors/asn1/ros/packet-ros-template.c due to improper validation of user-supplied input passed as an OID string. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. This issue only affects version 2.2.x. (CVE-2017-9347)
- An out-of-bounds read error exists in the OALMarshal_UncompressValue() function within file epan/dissectors/packet-dof.c when handling Distributed Object Framework (DOF) packets. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. This issue only affects version 2.2.x. (CVE-2017-9348)
- An infinite loop condition exists in the dissect_dcm_pdu_data() function within file epan/dissectors/packet-dcm.c when handling packets or packet trace files. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2017-9349)
- A memory allocation issue exists in the dissect_opensafety_ssdo_message() function within file epan/dissectors/packet-opensafety.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. (CVE-2017-9350)
- An out-of-bounds read error exists in the bootp_option() function within file epan/dissectors/packet-bootp.c when handling vendor class identifier strings in bootp packets due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition.
(CVE-2017-9351)
- An infinite loop condition exists in the get_bzr_pdu_len() function within file epan/dissectors/packet-bzr.c when handling packets or packet trace files. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2017-9352)
- A NULL pointer dereference flaw exists in the dissect_routing6_rpl() function within file epan/dissectors/packet-ipv6.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. This issue only affects version 2.2.x. (CVE-2017-9353)
- A NULL pointer dereference flaw exists in the dissect_rgmp() function within file epan/dissectors/packet-rgmp.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a specially crafted packet or packet trace file, to cause a denial of service condition. (CVE-2017-9354)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/docs/relnotes/wireshark-2.0.13.html

https://www.wireshark.org/docs/relnotes/wireshark-2.2.7.html

https://www.wireshark.org/security/wnpa-sec-2017-33.html

https://www.wireshark.org/security/wnpa-sec-2017-32.html

https://www.wireshark.org/security/wnpa-sec-2017-31.html

https://www.wireshark.org/security/wnpa-sec-2017-30.html

https://www.wireshark.org/security/wnpa-sec-2017-29.html

https://www.wireshark.org/security/wnpa-sec-2017-28.html

https://www.wireshark.org/security/wnpa-sec-2017-27.html

https://www.wireshark.org/security/wnpa-sec-2017-26.html

https://www.wireshark.org/security/wnpa-sec-2017-25.html

https://www.wireshark.org/security/wnpa-sec-2017-24.html

https://www.wireshark.org/security/wnpa-sec-2017-23.html

https://www.wireshark.org/security/wnpa-sec-2017-22.html

Solution

Upgrade to Wireshark version 2.0.13 / 2.2.7 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (E:P/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

6.1 (E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-9354
CVE	CVE-2017-9353
CVE	CVE-2017-9352
CVE	CVE-2017-9351
CVE	CVE-2017-9350
CVE	CVE-2017-9349
CVE	CVE-2017-9348
CVE	CVE-2017-9347
CVE	CVE-2017-9346
CVE	CVE-2017-9345
CVE	CVE-2017-9344

CVE	CVE-2017-9343
BID	98808
BID	98806
BID	98805
BID	98804
BID	98803
BID	98802
BID	98801
BID	98800
BID	98799
BID	98798
BID	98797
BID	98796

Plugin Information:

Publication date: 2017/06/07, Modification date: 2018/08/07

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.7
```

99437 (1) - Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.12 or 2.2.x prior to 2.2.6. It is, therefore, affected by multiple denial of service vulnerabilities :
- An infinite loop condition condition exists in the NetScaler file parser within file wiretap/netscaler.c when handling specially crafted capture files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7700)
- An infinite loop condition condition exists in the BGP dissector within file epan/dissectors/packet-bgp.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7701)
- An infinite loop condition condition exists in the WBXML dissector within file epan/dissectors/packet-wbxml.c when handling specially crafted packets or trace files.
An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7702)
- A denial of service vulnerability exists in the IMAP dissector within file epan/dissectors/packet-imap.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to crash the program. (CVE-2017-7703)
- An infinite loop condition condition exists in the DOF dissector within file epan/dissectors/packet-dof.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. Note that this issue only applies to the 2.2.x version. (CVE-2017-7704)
- An infinite loop condition condition exists in the RPC over RDMA dissector within file epan/dissectors/packet-rpcrdma.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7705)
- An infinite loop condition condition exists in the SIGCOMP dissector within file epan/dissectors/packet-sigcomp.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7745)
- An infinite loop condition condition exists in the SLSK dissector in the dissect_slsk_pdu() function within file epan/dissectors/packet-slsk.c, when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7746)
- An out-of-bounds read error exists in the PacketBB dissector in the dissect_pbb_addressblock() function within file epan/dissectors/packet-packetbb.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to crash the program. (CVE-2017-7747)
- An infinite loop condition condition exists in the WSP dissector within file epan/dissectors/packet-wsp.c when handling specially crafted packets or trace files. An unauthenticated, remote attacker can exploit this to cause excessive consumption of CPU resources, resulting in a denial of service condition. (CVE-2017-7748)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/docs/relnotes/wireshark-2.0.12.html

https://www.wireshark.org/docs/relnotes/wireshark-2.2.6.html

https://www.wireshark.org/security/wnpa-sec-2017-12.html

https://www.wireshark.org/security/wnpa-sec-2017-13.html

https://www.wireshark.org/security/wnpa-sec-2017-14.html

https://www.wireshark.org/security/wnpa-sec-2017-15.html

https://www.wireshark.org/security/wnpa-sec-2017-16.html

https://www.wireshark.org/security/wnpa-sec-2017-17.html

https://www.wireshark.org/security/wnpa-sec-2017-18.html

https://www.wireshark.org/security/wnpa-sec-2017-19.html

https://www.wireshark.org/security/wnpa-sec-2017-20.html

https://www.wireshark.org/security/wnpa-sec-2017-21.html

Solution

Upgrade to Wireshark version 2.0.12 / 2.2.6 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-7748
CVE	CVE-2017-7747
CVE	CVE-2017-7746
CVE	CVE-2017-7745
CVE	CVE-2017-7705
CVE	CVE-2017-7704
CVE	CVE-2017-7703
CVE	CVE-2017-7702
CVE	CVE-2017-7701
CVE	CVE-2017-7700
BID	97638
BID	97636
BID	97635
BID	97634
BID	97633
BID	97632
BID	97631
BID	97630
BID	97628

BID	97627

Plugin Information:

Publication date: 2017/04/18, Modification date: 2023/03/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.6
```

240237 (1) - SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities

Synopsis

The remote host is missing multiple security updates.

Description

The version of SQLite installed on the remote host is 3.44.0 through 3.49.0 before 3.49.1. It is, therefore, affected by multiple vulnerabilities:
- In SQLite 3.44.0 through 3.49.0 before 3.49.1, the concat_ws() SQL function can cause memory to be written beyond the end of a malloc-allocated buffer. If the separator argument is attacker-controlled and has a large string (e.g., 2MB or more), an integer overflow occurs in calculating the size of the result buffer, and thus malloc may not allocate enough memory. (CVE-2025-29087)
- An integer overflow can be triggered in SQLite's `concat_ws()` function. The resulting, truncated integer is then used to allocate a buffer. When SQLite then writes the resulting string to the buffer, it uses the original, untruncated size and thus a wild Heap Buffer overflow of size ~4GB can be triggered. This can result in arbitrary code execution. (CVE-2025-3277)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.sqlite.org/cves.html

Solution

Upgrade to SQLite 3.49.1 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

6.7

CVSS Base Score

7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

CVE	CVE-2025-3277
CVE	CVE-2025-29087

Plugin Information:

Publication date: 2025/06/23, Modification date: 2025/06/23

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe\sqlite3.dll
Installed version : 3.46.1.0
Fixed version     : 3.49.1
```

111387 (1) - Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.16, 2.4.x prior to 2.4.8, or 2.6.x prior to 2.6.2.
It is, therefore, affected by multiple vulnerabilities.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-34.html

https://www.wireshark.org/security/wnpa-sec-2018-35.html

https://www.wireshark.org/security/wnpa-sec-2018-36.html

https://www.wireshark.org/security/wnpa-sec-2018-37.html

https://www.wireshark.org/security/wnpa-sec-2018-38.html

https://www.wireshark.org/security/wnpa-sec-2018-39.html

https://www.wireshark.org/security/wnpa-sec-2018-40.html

https://www.wireshark.org/security/wnpa-sec-2018-41.html

https://www.wireshark.org/security/wnpa-sec-2018-42.html

https://www.wireshark.org/security/wnpa-sec-2018-43.html

Solution

Upgrade to Wireshark version 2.2.16 / 2.4.8 / 2.6.2 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (E:P/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

6.1 (E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-14370
CVE	CVE-2018-14369
CVE	CVE-2018-14368
CVE	CVE-2018-14367
CVE	CVE-2018-14344

CVE	CVE-2018-14343
CVE	CVE-2018-14342
CVE	CVE-2018-14341
CVE	CVE-2018-14340
CVE	CVE-2018-14339
BID	104847

Plugin Information:

Publication date: 2018/07/27, Modification date: 2024/09/02

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.16
```

193266 (1) - Security Updates Outlook for Windows (April 2024)

Synopsis

The Microsoft Outlook application installed on the remote host is missing a security update.

Description

The Microsoft Outlook application installed on the remote host is missing a security update. It is, therefore, affected by a spoofing vulnerability. External attackers could send specially crafted emails that will cause a connection from the victim to an untrusted location of attackers' control. This will leak the Net-NTLMv2 hash of the victim to the untrusted network which an attacker can then relay to another service and authenticate as the victim.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?02d9198f

Solution

Microsoft has released KB5002574 to address this issue.

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.2

CVSS v3.0 Base Score

8.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.1 (E:U/RL:O/RC:C)

CVSS Base Score

9.4 (AV:N/AC:L/Au:N/C:C/I:C/A:N)

CVSS Temporal Score

7.0 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-20670
XREF	IAVA-2024-A-0225-S
XREF	MSFT-MS24-5002574
XREF	MSKB-5002574

Plugin Information:

Publication date: 2024/04/12, Modification date: 2024/07/30

Assets

lognpacific3286 (TCP/0) Vulnerability State: Active

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.OutlookForWindows_1.0.0.0_neutral__8wekyb3d8bbwe
  Installed version : 1.0.0.0
  Fixed version     : 1.2023.0322.0100
```

81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

https://www.smacktls.com/#freak

https://www.openssl.org/news/secadv/20150108.txt

http://www.nessus.org/u?b78da2c4

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

1.4

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.2 (E:U/RL:OF/RC:C)

References

CVE	CVE-2015-0204
BID	71936
XREF	CERT-243585

Plugin Information:

Publication date: 2015/03/04, Modification date: 2021/02/03

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    EXP-RC4-MD5                   0x00, 0x03       RSA           RSA       RC4(40)
 MD5       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

157288 (1) - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE-327

Plugin Information:

Publication date: 2022/04/04, Modification date: 2024/05/14

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.1

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information:

Publication date: 2009/11/23, Modification date: 2025/02/12

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      ---------------------
---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

96765 (1) - Wireshark 2.0.x < 2.0.10 / 2.2.x < 2.2.4 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.10 or 2.2.x prior to 2.2.4. It is, therefore, affected by multiple denial of service vulnerabilities :
- A denial of service vulnerability exists when handling DHCPv6 packets due to an integer overflow condition in file epan/dissectors/packet-dhcpv6.c. An unauthenticated, remote attacker can exploit this to cause the program to enter a large loop that consumes excessive CPU resources (CVE-2017-5597).
- A denial of service vulnerability exists in the asterix_fspec_len() function within file epan/dissectors/packet-asterix.c due to an infinite loop flaw that is triggered because certain input is improperly validated. An unauthenticated, remote attacker can exploit this to consume excessive CPU resources (CVE-2017-5596).
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/security/wnpa-sec-2017-01.html

https://www.wireshark.org/security/wnpa-sec-2017-02.html

Solution

Upgrade to Wireshark version 2.0.10 / 2.2.4 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-5597
CVE	CVE-2017-5596

Plugin Information:

Publication date: 2017/01/25, Modification date: 2023/03/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.4
```

107093 (1) - Wireshark 2.2.x < 2.2.13 / 2.4.x < 2.4.5 Multiple DoS Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.13 or 2.4.x prior to 2.4.5. It is, therefore, affected by multiple denial of service vulnerabilities.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-05.html

https://www.wireshark.org/security/wnpa-sec-2018-06.html

https://www.wireshark.org/security/wnpa-sec-2018-07.html

https://www.wireshark.org/security/wnpa-sec-2018-08.html

https://www.wireshark.org/security/wnpa-sec-2018-09.html

https://www.wireshark.org/security/wnpa-sec-2018-10.html

https://www.wireshark.org/security/wnpa-sec-2018-11.html

https://www.wireshark.org/security/wnpa-sec-2018-12.html

https://www.wireshark.org/security/wnpa-sec-2018-13.html

https://www.wireshark.org/security/wnpa-sec-2018-14.html

Solution

Upgrade to Wireshark version 2.2.13 / 2.4.5 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (E:P/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.9 (E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-7337
CVE	CVE-2018-7336
CVE	CVE-2018-7335
CVE	CVE-2018-7334
CVE	CVE-2018-7333
CVE	CVE-2018-7332

CVE	CVE-2018-7331
CVE	CVE-2018-7330
CVE	CVE-2018-7329
CVE	CVE-2018-7328
CVE	CVE-2018-7327
CVE	CVE-2018-7326
CVE	CVE-2018-7325
CVE	CVE-2018-7324
CVE	CVE-2018-7323
CVE	CVE-2018-7322
CVE	CVE-2018-7321
CVE	CVE-2018-7320
BID	103166
BID	103165
BID	103164
BID	103162
BID	103160
BID	103158

Plugin Information:

Publication date: 2018/03/01, Modification date: 2025/10/27

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.13
```

108885 (1) - Wireshark 2.2.x < 2.2.14 / 2.4.x < 2.4.6 Multiple Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.14 or 2.4.x prior to 2.4.6. It is, therefore, affected by multiple vulnerabilities.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-15.html

https://www.wireshark.org/security/wnpa-sec-2018-16.html

https://www.wireshark.org/security/wnpa-sec-2018-17.html

https://www.wireshark.org/security/wnpa-sec-2018-18.html

https://www.wireshark.org/security/wnpa-sec-2018-19.html

https://www.wireshark.org/security/wnpa-sec-2018-20.html

https://www.wireshark.org/security/wnpa-sec-2018-21.html

https://www.wireshark.org/security/wnpa-sec-2018-22.html

https://www.wireshark.org/security/wnpa-sec-2018-23.html

https://www.wireshark.org/security/wnpa-sec-2018-24.html

Solution

Upgrade to Wireshark version 2.2.14 / 2.4.6 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (E:P/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.9 (E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-9274
CVE	CVE-2018-9273
CVE	CVE-2018-9272
CVE	CVE-2018-9271
CVE	CVE-2018-9270
CVE	CVE-2018-9269

CVE	CVE-2018-9268
CVE	CVE-2018-9267
CVE	CVE-2018-9266
CVE	CVE-2018-9265
CVE	CVE-2018-9264
CVE	CVE-2018-9263
CVE	CVE-2018-9262
CVE	CVE-2018-9261
CVE	CVE-2018-9260
CVE	CVE-2018-9259
CVE	CVE-2018-9258
CVE	CVE-2018-9257
CVE	CVE-2018-9256
CVE	CVE-2017-9616
BID	99085

Plugin Information:

Publication date: 2018/04/06, Modification date: 2024/11/14

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.14
```

117339 (1) - Wireshark 2.2.x < 2.2.17 / 2.4.x < 2.4.9 / 2.6.x < 2.6.3 Multiple Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.17, 2.4.x prior to 2.4.9, or 2.6.x prior to 2.6.3.
It is, therefore, affected by multiple vulnerabilities.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-44.html

https://www.wireshark.org/security/wnpa-sec-2018-45.html

https://www.wireshark.org/security/wnpa-sec-2018-46.html

Solution

Upgrade to Wireshark version 2.2.17 / 2.4.9 / 2.6.3 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-16058
CVE	CVE-2018-16057
CVE	CVE-2018-16056
BID	105174

Plugin Information:

Publication date: 2018/09/07, Modification date: 2024/08/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.17
```

106142 (1) - Wireshark 2.2.x < 2.2.12 / 2.4.x < 2.4.4 DoS Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.12 or 2.4.x prior to 2.4.4. It is, therefore, affected by a denial of service vulnerability.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-01.html

https://www.wireshark.org/security/wnpa-sec-2018-03.html

https://www.wireshark.org/security/wnpa-sec-2018-04.html

Solution

Upgrade to Wireshark version 2.2.12 / 2.4.4 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-5336
CVE	CVE-2018-5335
CVE	CVE-2018-5334
CVE	CVE-2017-17997
BID	102504
BID	102500
BID	102499

Plugin Information:

Publication date: 2018/01/18, Modification date: 2019/11/08

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.12
```

110269 (1) - Wireshark 2.2.x < 2.2.15 / 2.4.x < 2.4.7 / 2.6.x < 2.6.1 Multiple Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.15, 2.4.x prior to 2.4.6, or 2.6.x prior to 2.6.1.
It is, therefore, affected by multiple vulnerabilities.

See Also

https://www.wireshark.org/security/wnpa-sec-2018-25.html

https://www.wireshark.org/security/wnpa-sec-2018-26.html

https://www.wireshark.org/security/wnpa-sec-2018-27.html

https://www.wireshark.org/security/wnpa-sec-2018-28.html

https://www.wireshark.org/security/wnpa-sec-2018-29.html

https://www.wireshark.org/security/wnpa-sec-2018-30.html

https://www.wireshark.org/security/wnpa-sec-2018-31.html

https://www.wireshark.org/security/wnpa-sec-2018-32.html

https://www.wireshark.org/security/wnpa-sec-2018-33.html

Solution

Upgrade to Wireshark version 2.2.15 / 2.4.7 / 2.6.1 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-11362
CVE	CVE-2018-11361
CVE	CVE-2018-11360
CVE	CVE-2018-11359
CVE	CVE-2018-11358
CVE	CVE-2018-11357

CVE	CVE-2018-11356
CVE	CVE-2018-11355
CVE	CVE-2018-11354
BID	104308

Plugin Information:

Publication date: 2018/05/31, Modification date: 2019/11/04

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.15
```

51192 (1) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2025/06/16

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=LogNPacific3286
|-Issuer  : CN=LogNPacific3286
```

95435 (1) - Wireshark 2.0.x < 2.0.8 / 2.2.x < 2.2.2 Multiple DoS

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.0.x prior to 2.0.8 or 2.2.x prior to 2.2.2. It is, therefore, affected by multiple denial of service vulnerabilities :
- A flaw exists in the dissect_PNIO_C_SDU_RTC1() function in packet-pn-rtc-one.c that causes excessive looping. An unauthenticated, remote attacker can exploit this, via specially crafted network traffic or a specially crafted capture file, to exhaust available resources. Note that this vulnerability only affects 2.2.x versions.
(CVE-2016-9372)
- A use-after-free error exists in the DCEPRC dissector due to improper handling of IA5 SMS decoding. An unauthenticated, remote attacker can exploit this, via specially crafted network traffic or a specially crafted capture file, to cause the application to crash.
(CVE-2016-9373)
- A buffer over-read flaw exists in the AllJoyn dissector due to improper handling of signature lengths. An unauthenticated, remote attacker can exploit this, via specially crafted network traffic or a specially crafted capture file, to cause the application to crash.
(CVE-2016-9374)
- A flaw exists in the DTN dissector in the display_metadata_block() function due to improper SDNV evaluation. An unauthenticated, remote attacker can exploit this, via specially crafted network traffic or a specially crafted capture file, to cause an infinite loop. (CVE-2016-9375)
- Multiple flaws exist in the OpenFlow dissector in packet-openflow_v5.c due to improper handling of too short data lengths. An unauthenticated, remote attacker can exploit this, via specially crafted network traffic or a specially crafted capture file, to cause the application to crash. (CVE-2016-9376)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/security/wnpa-sec-2016-58.html

https://www.wireshark.org/security/wnpa-sec-2016-59.html

https://www.wireshark.org/security/wnpa-sec-2016-60.html

https://www.wireshark.org/security/wnpa-sec-2016-61.html

https://www.wireshark.org/security/wnpa-sec-2016-62.html

Solution

Upgrade to Wireshark version 2.0.8 / 2.2.2 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.2 (E:U/RL:O/RC:C)

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.2 (E:U/RL:OF/RC:C)

References

CVE	CVE-2016-9376

CVE	CVE-2016-9375
CVE	CVE-2016-9374
CVE	CVE-2016-9373
CVE	CVE-2016-9372
BID	94369
BID	94368

Plugin Information:

Publication date: 2016/12/01, Modification date: 2023/03/09

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.2
```

57582 (1) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2022/06/14

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=LogNPacific3286
```

176372 (1) - Wireshark 2.2.x < 2.2.17 Multiple Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is prior to 2.2.17. It is, therefore, affected by multiple vulnerabilities as referenced in the wireshark-2.2.17 advisory.
- In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Bluetooth AVDTP dissector could crash. This was addressed in epan/dissectors/packet-btavdtp.c by properly initializing a data structure.
(CVE-2018-16058)
- In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Bluetooth Attribute Protocol dissector could crash. This was addressed in epan/dissectors/packet-btatt.c by verifying that a dissector for a specific UUID exists.
(CVE-2018-16056)
- In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Radiotap dissector could crash. This was addressed in epan/dissectors/packet-ieee80211-radiotap-iter.c by validating iterator operations.
(CVE-2018-16057)
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/docs/relnotes/wireshark-2.2.17.html

https://gitlab.com/wireshark/wireshark/-/issues/14884

https://www.wireshark.org/security/wnpa-sec-2018-44

https://gitlab.com/wireshark/wireshark/-/issues/14994

https://www.wireshark.org/security/wnpa-sec-2018-45

https://gitlab.com/wireshark/wireshark/-/issues/15022

https://www.wireshark.org/security/wnpa-sec-2018-46

Solution

Upgrade to Wireshark version 2.2.17 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2018-16058
CVE	CVE-2018-16057

CVE	CVE-2018-16056
XREF	IAVB-2018-B-0120-S

Plugin Information:

Publication date: 2023/05/25, Modification date: 2023/05/25

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.17
```

104743 (1) - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE-327

Plugin Information:

Publication date: 2017/11/22, Modification date: 2023/04/19

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
TLSv1 is enabled and the server supports at least one cipher.
```

26928 (1) - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?6527892d

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE-934
XREF	CWE-928
XREF	CWE-803
XREF	CWE-753
XREF	CWE-720
XREF	CWE-327
XREF	CWE-326

Plugin Information:

Publication date: 2007/10/08, Modification date: 2021/02/03

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    EXP1024-DES-CBC-SHA           0x00, 0x62       RSA           RSA       DES-CBC(56)
 SHA1      export
    EXP1024-RC4-SHA               0x00, 0x64       RSA           RSA       RC4(56)
 SHA1      export
    EXP-RC4-MD5                   0x00, 0x03       RSA           RSA       RC4(40)
 MD5       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA       DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
```

```
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 (1) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.3

CVSS v3.0 Base Score

5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (E:U/RL:X/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (E:U/RL:ND/RC:C)

References

CVE	CVE-2015-2808
CVE	CVE-2013-2566
BID	73684
BID	58796

Plugin Information:

Publication date: 2013/04/05, Modification date: 2025/05/09

Assets

lognpacific3286 (TCP/3389) Vulnerability State: Active

```
List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)
```

```
   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   EXP1024-RC4-SHA               0x00, 0x64      RSA          RSA      RC4(56)
SHA1      export
   EXP-RC4-MD5                   0x00, 0x03      RSA          RSA      RC4(40)
MD5       export

 Unrecognized Ciphers

   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   TLS1_CK_RSA_WITH_RC4_128_MD5
   TLS1_CK_RSA_WITH_RC4_128_SHA

The fields above are :

 {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 Auth={authentication}
 Encrypt={symmetric encryption method}
 MAC={message authentication code}
 {export flag}
```

105007 (1) - Wireshark 2.2.x < 2.2.11 / 2.4.x < 2.4.3 DoS Vulnerabilities

Synopsis

An application installed on the remote Windows host is affected by multiple denial of service vulnerabilities.

Description

The version of Wireshark installed on the remote Windows host is 2.2.x prior to 2.2.11 or 2.4.x prior to 2.4.3. It is, therefore, affected by denial of service vulnerabilities in the IWARP_MPA, NetBIOS, and CIP Safety dissectors. An unauthenticated, remote attacker can exploit this by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://www.wireshark.org/security/wnpa-sec-2017-47.html

https://www.wireshark.org/security/wnpa-sec-2017-48.html

https://www.wireshark.org/security/wnpa-sec-2017-49.html

Solution

Upgrade to Wireshark version 2.2.11 / 2.4.3 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (E:P/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.9 (E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-17085
CVE	CVE-2017-17084
CVE	CVE-2017-17083

Plugin Information:

Publication date: 2017/12/01, Modification date: 2019/11/12

Assets

lognpacific3286 (TCP/445) Vulnerability State: Active

```
Path              : C:\Program Files\Wireshark
Installed version : 2.2.1
Fixed version     : 2.2.11
```

264898 (1) - Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)

Synopsis

Microsoft Teams for Desktop is affected by an elevation of privilege vulnerability.

Description

The version of Microsoft Teams for Desktop on the remote Windows host is prior to 25163.3611.3774.6315 It is, therefore, affected by an elevation of privilege vulnerability:
- Improper handling of insufficient permissions or privileges in Microsoft Teams allows an authorized attacker to elevate privileges over a network. (CVE-2025-49731)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?705592ec

Solution

Upgrade to Microsoft Teams for Desktop version 25163.3611.3774.6315 or later via the Microsoft Store.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

1.4

CVSS v3.0 Base Score

3.1 (AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

STIG Severity

I

References

CVE	CVE-2025-49731
XREF	IAVA-2025-A-0493-S

Plugin Information:

Publication date: 2025/09/16, Modification date: 2025/10/29

Assets

lognpacific3286 (TCP/0) Vulnerability State: Active

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 25163.3611.3774.6315
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.2

CVSS Base Score

2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE-200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2024/10/07

Assets

lognpacific3286 (ICMP/0) Vulnerability State: Active

```
The ICMP timestamps seem to be in little endian format (not in network format)
The remote clock is synchronized with the local clock.
```

Assets Summary (Executive)

lognpacific3286

Summary

Critical	High	Medium	Low	Info	Total
3	12	17	2	0	34

Details

Severity	Plugin Id	Name
Critical	213824	Wireshark SEoL (2.2.x)
Critical	242325	SQLite < 3.50.2 Memory Corruption
Critical	56710	Wireshark / Ethereal Unsupported Version Detection
High	97574	Wireshark 2.0.x < 2.0.11 / 2.2.x < 2.2.5 Multiple DoS
High	101898	Wireshark 2.0.x < 2.0.14 / 2.2.x < 2.2.8 Multiple DoS
High	103569	Windows Defender Antimalware/Antivirus Signature Definition Check
High	250276	Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025)
High	103985	Wireshark 2.2.x < 2.2.10 Multiple DoS
High	102920	Wireshark 2.2.x < 2.2.9 Multiple DoS
High	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
High	100671	Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS
High	99437	Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS
High	240237	SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities
High	111387	Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities
High	193266	Security Updates Outlook for Windows (April 2024)
Medium	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium	157288	TLS Version 1.1 Deprecated Protocol
Medium	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
Medium	96765	Wireshark 2.0.x < 2.0.10 / 2.2.x < 2.2.4 Multiple DoS
Medium	107093	Wireshark 2.2.x < 2.2.13 / 2.4.x < 2.4.5 Multiple DoS Vulnerabilities
Medium	108885	Wireshark 2.2.x < 2.2.14 / 2.4.x < 2.4.6 Multiple Vulnerabilities
Medium	117339	Wireshark 2.2.x < 2.2.17 / 2.4.x < 2.4.9 / 2.6.x < 2.6.3 Multiple Vulnerabilities
Medium	106142	Wireshark 2.2.x < 2.2.12 / 2.4.x < 2.4.4 DoS Vulnerabilities
Medium	110269	Wireshark 2.2.x < 2.2.15 / 2.4.x < 2.4.7 / 2.6.x < 2.6.1 Multiple Vulnerabilities

Medium	51192	SSL Certificate Cannot Be Trusted
Medium	95435	Wireshark 2.0.x < 2.0.8 / 2.2.x < 2.2.2 Multiple DoS
Medium	57582	SSL Self-Signed Certificate
Medium	176372	Wireshark 2.2.x < 2.2.17 Multiple Vulnerabilities
Medium	104743	TLS Version 1.0 Protocol Detection
Medium	26928	SSL Weak Cipher Suites Supported
Medium	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium	105007	Wireshark 2.2.x < 2.2.11 / 2.4.x < 2.4.3 DoS Vulnerabilities
Low	264898	Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2025)
Low	10114	ICMP Timestamp Request Remote Date Disclosure

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 88% of the vulnerabilities on the network:

Action to take	Vulns	Assets
Wireshark 2.2.x < 2.2.17 Multiple Vulnerabilities: Upgrade to Wireshark version 2.2.17 or later.	112	1
SQLite < 3.50.2 Memory Corruption: Upgrade to SQLite 3.50.2 or later.	3	1
Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (August 2025): Upgrade to Microsoft Teams for Desktop version 25122.1415.3698.6812 or later via the Microsoft Store.	2	1

Audits FAILED

WN11-00-000031 - Windows 11 systems must use a BitLocker PIN for pre-boot authentication.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. Pre-boot authentication prevents unauthorized users from accessing encrypted drives.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives 'Require additional authentication at startup' to 'Enabled' with 'Configure TPM Startup PIN:' set to 'Require startup PIN with TPM' or with 'Configure TPM startup key and PIN:' set to 'Require startup key and PIN with TPM'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28(1)
800-53R5	SC-28(1)
CAT	I
CCI	CCI-002476
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.33
ITSG-33	SC-28(1)
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2

QCSC-V1	6.2
RULE-ID	SV-253260r958872_rule
STIG-ID	WN11-00-000031
TBA-FIISB	28.1
VULN-ID	V-253260

Assets

lognpacific3286

```
The following AND condition has failed:
{
 UseAdvancedStartup:
 Remote value: NULL
 Policy value: 1
}
```

WN11-00-000032 - Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. Pre-boot authentication prevents unauthorized users from accessing encrypted drives. Increasing the pin length requires a greater number of guesses for an attacker.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives 'Configure minimum PIN length for startup' to 'Enabled' with 'Minimum characters:' set to '6' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	IA-8
800-53R5	IA-8
CAT	II
CCI	CCI-000804
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-8
ITSG-33	IA-8a.
NESA	T4.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253261r958504_rule

STIG-ID	WN11-00-000032
SWIFT-CSCV1	2.8
VULN-ID	V-253261

Assets

lognpacific3286

```
NULL
```

WN11-00-000090 - Accounts must be configured to require password expiration.

Info

Passwords that do not expire increase exposure with a greater probability of being discovered or cracked.

Solution

Configure all passwords to expire.
Run 'Computer Management'.
Navigate to System Tools >> Local Users and Groups >> Users.
Double-click each active account.
Ensure 'Password never expires' is not checked on all active accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20

NIAV2	AM21
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253273r1051040_rule
STIG-ID	WN11-00-000090
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253273

Assets

lognpacific3286

```
'Name  SID
----  ---
Guest S-1-5-21-108538807-2850267539-2289239689-501'
```

WN11-00-000125 - Copilot in Windows must be disabled for Windows 11

Info

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 uncontrolled updates to the system.

Solution

Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Windows Copilot >> 'Turn off Windows Copilot' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2
RULE-ID	SV-268317r1016371_rule

STIG-ID	WN11-00-000125
SWIFT-CSCV1	2.3
VULN-ID	V-268317

Assets

lognpacific3286

```
Non-compliant items:
  HKU\S-1-5-21-108538807-2850267539-2289239689-500\Software\Policies\Microsoft\Windows
\WindowsCopilot -
```

WN11-00-000135 - A host-based firewall must be installed and enabled on the system.

Info

A firewall provides a line of defense against attack, allowing or blocking inbound and outbound connections based on a set of rules.

Solution

Install and enable a host-based firewall on the system.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253281r991589_rule
STIG-ID	WN11-00-000135
SWIFT-CSCV1	2.3
VULN-ID	V-253281

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Domain:
 Remote value: NULL
 Policy value: 1


-------------------------
```

```
FAILED - PrivateProfile:
 Remote value: NULL
 Policy value: 1


-------------------------
FAILED - PublicProfile:
 Remote value: NULL
 Policy value: 1
```

WN11-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut.

Info

Attackers are constantly looking for vulnerabilities in systems and applications. Data Execution Prevention (DEP) prevents harmful code from running in protected memory locations reserved for Windows and other programs.

Solution

Configure DEP to at least OptOut.
Note: Suspend BitLocker before making changes to the DEP configuration.
Open a command prompt (cmd.exe) or PowerShell with elevated privileges (Run as administrator).
Enter 'BCDEDIT /set {current} nx OptOut'. (If using PowerShell '{current}' must be enclosed in quotes.) 'AlwaysOn', a more restrictive selection, is also valid but does not allow applications that do not function properly to be opted out of DEP.
Opted out exceptions can be configured in the 'System Properties'.
Open 'System' in Control Panel.
Select 'Advanced system settings'.
Click 'Settings' in the 'Performance' section.
Select the 'Data Execution Prevention' tab.
Applications that are opted out are configured in the window below the selection 'Turn on DEP for all programs and services except those I select:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	I
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-253283r958928_rule
STIG-ID	WN11-00-000145
VULN-ID	V-253283

Assets

lognpacific3286

```
'nx                    OptIn'
```

WN11-00-000150 - Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.

Info

Attackers are constantly looking for vulnerabilities in systems and applications. Structured Exception Handling Overwrite Protection (SEHOP) blocks exploits that use the Structured Exception Handling overwrite technique, a common buffer overflow attack.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	I
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-253284r958928_rule
STIG-ID	WN11-00-000150
VULN-ID	V-253284

Assets

lognpacific3286

NULL

WN11-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system.

Info

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

Solution

Disable 'Windows PowerShell 2.0' on the system.
Run 'Windows PowerShell' with elevated privileges (run as administrator).
Enter the following:
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root
This command must disable both 'MicrosoftWindowsPowerShellV2Root' and 'MicrosoftWindowsPowerShellV2' which correspond to 'Windows PowerShell 2.0' and 'Windows PowerShell 2.0 Engine' respectively in 'Turn Windows features on or off'.
Alternately:
Search for 'Features'.
Select 'Turn Windows features on or off'.
De-select 'Windows PowerShell 2.0'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253285r958478_rule
STIG-ID	WN11-00-000155
SWIFT-CSCV1	2.3
VULN-ID	V-253285

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - PowerShellv2:
 POWERSHELL_NO_RESULT: powershell command returned no result



-------------------------
FAILED - PowerShellv2Root:
 POWERSHELL_NO_RESULT: powershell command returned no result
```

WN11-00-000175 - The Secondary Logon service must be disabled on Windows 11.

Info

The Secondary Logon service provides a means for entering alternate credentials, typically used to run commands with elevated privileges. Using privileged credentials in a standard user session can expose those credentials to theft.

Solution

Configure the 'Secondary Logon' service 'Startup Type' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253289r958478_rule
STIG-ID	WN11-00-000175
SWIFT-CSCV1	2.3
VULN-ID	V-253289

Assets

lognpacific3286

```
'manual'
```

WN11-00-000260 - The Windows 11 time service must synchronize with an appropriate DOD time source.

Info

The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. If the Windows Time Service is used, it must synchronize with a secure, authorized time source. Domain-joined systems are automatically configured to synchronize with domain controllers. If an NTP server is configured, it must synchronize with a secure, authorized time source.

Solution

Configure the system to synchronize time with an appropriate DOD time source.
Domain-joined systems use NT5DS to synchronize time from other systems in the domain by default.
If the system needs to be configured to an NTP server, configure the system to point to an authorized time server by setting the policy value for Computer Configuration >> Administrative Templates >> System >> Windows Time Service >> Time Providers >> 'Configure Windows NTP Client' to 'Enabled', and configure the 'NtpServer' field to point to an appropriate DOD time server.
The US Naval Observatory operates stratum 1 time servers, identified at https://www.cnmoc.usff.navy.mil/Our-Commands/United-States-Naval-Observatory/Precise-Time-Department/Network-Time-Protocol-NTP/. Time synchronization will occur through a hierarchy of time servers down to the local level. Clients and lower-level servers will synchronize with an authorized time server in the hierarchy.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.7
800-171R3	03.03.07
800-53	AU-8(1)(a)
800-53R5	SC-45(1)(a)
CAT	III
CCI	CCI-001891
CCI	CCI-004923
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.17
ISO/IEC-27001	A.12.4.4
ITSG-33	AU-8(1)
NESA	T3.6.7
NIAV2	NS44
NIAV2	NS45

NIAV2	NS46
NIAV2	NS47
PCI-DSSV3.2.1	10.4
PCI-DSSV3.2.1	10.4.1
PCI-DSSV3.2.1	10.4.3
PCI-DSSV4.0	10.6
PCI-DSSV4.0	10.6.1
PCI-DSSV4.0	10.6.2
PCI-DSSV4.0	10.6.3
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253296r1051041_rule
STIG-ID	WN11-00-000260
TBA-FIISB	37.4
VULN-ID	V-253296

Assets

lognpacific3286

```
'Type: NTP (Local)'
```

WN11-AC-000005 - Windows 11 account lockout duration must be configured to 15 minutes or greater.

Info

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

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> 'Account lockout duration' to '15' minutes or greater.
A value of '0' is also acceptable, requiring an administrator to unlock the account.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08b.
800-53	AC-7b.
800-53R5	AC-7b.
CAT	II
CCI	CCI-002238
CN-L3	7.1.2.7(f)
CN-L3	7.1.3.1(c)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7b.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.7
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253297r958736_rule
STIG-ID	WN11-AC-000005
TBA-FIISB	36.2.4
TBA-FIISB	45.1.2
VULN-ID	V-253297

Assets

lognpacific3286

```
10
```

WN11-AC-000010 - The number of allowed bad logon attempts must be configured to three or less.

Info

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 a normal user logon.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-53	AC-7a.
800-53R5	AC-7a.
CAT	II
CCI	CCI-000044
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253298r958388_rule
STIG-ID	WN11-AC-000010
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-253298

Assets

lognpacific3286

```
10
```

WN11-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes.

Info

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-53	AC-7a.
800-53R5	AC-7a.
CAT	II
CCI	CCI-000044
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253299r958388_rule
STIG-ID	WN11-AC-000015
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-253299

Assets

lognpacific3286

```
10
```

WN11-AC-000020 - The password history must be configured to 24 passwords remembered.

Info

A system is more vulnerable to unauthorized access when system users recycle the same password several times without being required to change a password 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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07b.
800-53	IA-5(1)(b)
800-53R5	IA-5(1)(b)
CAT	II
CCI	CCI-004061
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(b)
NESA	T5.2.3
NIAV2	AM22d
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253300r1000103_rule

STIG-ID	WN11-AC-000020
SWIFT-CSCV1	4.1
VULN-ID	V-253300

Assets

lognpacific3286

0

WN11-AC-000030 - The minimum password age must be configured to at least 1 day.

Info

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.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> 'Minimum Password Age' to at least '1' day.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000198
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21

QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253302r1051043_rule
STIG-ID	WN11-AC-000030
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253302

Assets

lognpacific3286

```
0
```

WN11-AC-000035 - Passwords must, at a minimum, be 14 characters.

Info

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07a.
800-53	IA-5(1)(a)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000205
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(a)
NESA	T5.2.3
NIAV2	AM19a
NIAV2	AM19b

NIAV2	AM19c
NIAV2	AM19d
NIAV2	AM22a
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253303r1051044_rule
STIG-ID	WN11-AC-000035
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-253303

Assets

lognpacific3286

```
0
```

WN11-AC-000040 - The built-in Microsoft password complexity filter must be enabled.

Info

The use of complex passwords increases their strength against guessing and brute-force attacks. This setting configures the system to verify that newly created passwords conform to the Windows password complexity policy.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.7
800-171R3	03.05.07a.
800-53	IA-5(1)(a)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000192
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(a)
NESA	T5.2.3
NIAV2	AM19a
NIAV2	AM19b

NIAV2	AM19c
NIAV2	AM19d
NIAV2	AM22a
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253304r1051045_rule
STIG-ID	WN11-AC-000040
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-253304

Assets

lognpacific3286

```
'disabled'
```

WN11-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253306r991570_rule
STIG-ID	WN11-AU-000005
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253306

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253307r991570_rule
STIG-ID	WN11-AU-000010
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253307

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000035 - The system must be configured to audit Account Management - User Account Management failures.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SI-11b.
800-53R5	SI-11b.
CAT	II
CCI	CCI-001314
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-11c.
RULE-ID	SV-253309r958566_rule
STIG-ID	WN11-AU-000035
VULN-ID	V-253309

Assets

lognpacific3286

```
'success'
```

WN11-AU-000045 - The system must be configured to audit Detailed Tracking - PNP Activity successes.

Info

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.
Plug and Play activity records events related to the successful connection of external devices.

Solution

Computer Configuration >> Windows Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> 'Audit PNP Activity' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.5
800-171R3	03.03.03a.
800-171R3	03.04.05
800-53	AU-12c.
800-53	CM-5(1)
800-53R5	AU-12c.
800-53R5	CM-5(1)(b)
CAT	II
CCI	CCI-000172
CCI	CCI-001814
CCI	CCI-003938
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7

CSF	PR.IP-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.4
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.19
ISO-27001-2022	A.8.31
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	CM-5(1)
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.6.1
NESA	T7.5.3
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2

QCSC-V1	7.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253311r1051047_rule
STIG-ID	WN11-AU-000045
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253311

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.5
800-171R3	03.03.03a.
800-171R3	03.04.05
800-53	AU-12c.
800-53	CM-5(1)
800-53R5	AU-12c.
800-53R5	CM-5(1)(b)
CAT	II
CCI	CCI-000172
CCI	CCI-001814
CCI	CCI-003938
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7

CSF	PR.IP-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.4
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.19
ISO-27001-2022	A.8.31
ISO-27001-2022	A.8.32
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	CM-5(1)
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.6.1
NESA	T7.5.3
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2

QCSC-V1	7.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253312r1051048_rule
STIG-ID	WN11-AU-000050
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253312

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000054 - The system must be configured to audit Logon/Logoff - Account Lockout failures.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253313r991578_rule
STIG-ID	WN11-AU-000054
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253313

Assets

lognpacific3286

```
'success'
```

WN11-AU-000060 - The system must be configured to audit Logon/Logoff - Group Membership successes.

Info

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

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> 'Audit Group Membership' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253314r991570_rule
STIG-ID	WN11-AU-000060
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253314

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000081 - Windows 11 must be configured to audit Object Access - File Share failures.

Info

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.
Auditing file shares records events related to connection to shares on a system including system shares such as C$.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File Share' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253319r991572_rule
STIG-ID	WN11-AU-000081
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253319

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000082 - Windows 11 must be configured to audit Object Access - File Share successes.

Info

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.
Auditing file shares records events related to connection to shares on a system including system shares such as C$.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit File Share' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253320r991572_rule
STIG-ID	WN11-AU-000082
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253320

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000083 - Windows 11 must be configured to audit Object Access - Other Object Access Events successes.

Info

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.
Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects.

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253321r991572_rule
STIG-ID	WN11-AU-000083
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253321

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000084 - Windows 11 must be configured to audit Object Access - Other Object Access Events failures.

Info

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.
Auditing for other object access records events related to the management of task scheduler jobs and COM+ objects.

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253322r991572_rule
STIG-ID	WN11-AU-000084
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253322

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000085 - The system must be configured to audit Object Access - Removable Storage failures.

Info

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.
Auditing object access for removable media records events related to access attempts on file system objects on removable storage devices.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Removable Storage' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253323r991583_rule
STIG-ID	WN11-AU-000085
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253323

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000090 - The system must be configured to audit Object Access - Removable Storage successes.

Info

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.
Auditing object access for removable media records events related to access attempts on file system objects on removable storage devices.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> 'Audit Removable Storage' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253324r991583_rule
STIG-ID	WN11-AU-000090
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253324

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253327r991572_rule
STIG-ID	WN11-AU-000107
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253327

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Sensitive Privilege Use records events related to use of sensitive privileges, such as 'Act as part of the operating system' or 'Debug programs'.

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07b.
800-53	AC-6(9)
800-53R5	AC-6(9)
CAT	II
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6

NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253328r958732_rule
STIG-ID	WN11-AU-000110
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253328

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Sensitive Privilege Use records events related to use of sensitive privileges, such as 'Act as part of the operating system' or 'Debug programs'.

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253329r991575_rule
STIG-ID	WN11-AU-000115
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253329

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000120 - The system must be configured to audit System - IPsec Driver failures.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253330r991586_rule
STIG-ID	WN11-AU-000120
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253330

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000150 - The system must be configured to audit System - Security System Extension successes.

Info

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

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253334r991575_rule
STIG-ID	WN11-AU-000150
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253334

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000500 - The Application event log size must be configured to 32768 KB or greater.

Info

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.

Solution

If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.
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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253337r958752_rule
STIG-ID	WN11-AU-000500
VULN-ID	V-253337

Assets

lognpacific3286

```
NULL
```

WN11-AU-000505 - The Security event log size must be configured to 1024000 KB or greater.

Info

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.

Solution

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 '1024000' or greater.
If the system is configured to send audit records directly to an audit server, this must be documented with the ISSO.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253338r958752_rule
STIG-ID	WN11-AU-000505
VULN-ID	V-253338

Assets

lognpacific3286

```
NULL
```

WN11-AU-000510 - The System event log size must be configured to 32768 KB or greater.

Info

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.

Solution

If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.
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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	AU-4
800-53R5	AU-4
CAT	II
CCI	CCI-001849
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.6
ITSG-33	AU-4
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253339r958752_rule
STIG-ID	WN11-AU-000510
VULN-ID	V-253339

Assets

lognpacific3286

```
NULL
```

WN11-AU-000550 - Windows 11 must be configured to audit Other Policy Change Events Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Policy Change Events contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253343r958412_rule
STIG-ID	WN11-AU-000550
SWIFT-CSCV1	6.4
VULN-ID	V-253343

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000555 - Windows 11 must be configured to audit Other Policy Change Events Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Policy Change Events contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253344r958412_rule
STIG-ID	WN11-AU-000555
SWIFT-CSCV1	6.4
VULN-ID	V-253344

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000560 - Windows 11 must be configured to audit other Logon/Logoff Events Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Logon/Logoff Events determines whether Windows generates audit events for other logon or logoff events. Logon events are essential to understanding user activity and detecting potential attacks.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253345r958412_rule
STIG-ID	WN11-AU-000560
SWIFT-CSCV1	6.4
VULN-ID	V-253345

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000565 - Windows 11 must be configured to audit other Logon/Logoff Events Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Other Logon/Logoff Events determines whether Windows generates audit events for other logon or logoff events. Logon events are essential to understanding user activity and detecting potential attacks.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253346r958412_rule
STIG-ID	WN11-AU-000565
SWIFT-CSCV1	6.4
VULN-ID	V-253346

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000570 - Windows 11 must be configured to audit Detailed File Share Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit Detailed File Share allows the user to audit attempts to access files and folders on a shared folder.
The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection established between a client and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> Audit Detailed File Share' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253347r958412_rule
STIG-ID	WN11-AU-000570
SWIFT-CSCV1	6.4
VULN-ID	V-253347

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000575 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Successes.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit MPSSVC Rule-Level Policy Change determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe).

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> Audit MPSSVC Rule-Level Policy Change' with 'Success' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253348r958412_rule
STIG-ID	WN11-AU-000575
SWIFT-CSCV1	6.4
VULN-ID	V-253348

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000580 - Windows 11 must be configured to audit MPSSVC Rule-Level Policy Change Failures.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Audit MPSSVC Rule-Level Policy Change determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe).

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Policy Change >> Audit MPSSVC Rule-Level Policy Change' with 'Failure' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3a.
CAT	II
CCI	CCI-000130
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253349r958412_rule
STIG-ID	WN11-AU-000580
SWIFT-CSCV1	6.4
VULN-ID	V-253349

Assets

lognpacific3286

```
'no auditing'
```

WN11-AU-000585 - Windows 11 must have command line process auditing events enabled for failures.

Info

When this policy setting is enabled, the operating system generates audit events when a process fails to start and the name of the program or user that created it.
These audit events can assist in understanding how a computer is being used and tracking user activity.

Solution

Go to Computer Configuration >> Windows Settings >>Security Settings>> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> Set 'Audit Process Creation' to 'Failure'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07b.
800-53	AC-6(9)
800-53R5	AC-6(9)
CAT	II
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-257770r958412_rule
STIG-ID	WN11-AU-000585
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-257770

Assets

lognpacific3286

```
'no auditing'
```

WN11-CC-000005 - Camera access from the lock screen must be disabled.

Info

Enabling camera access from the lock screen could allow for unauthorized use. Requiring logon will ensure the device is only used by authorized personnel.

Solution

If the device does not have a camera, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> 'Prevent enabling lock screen camera' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253350r958478_rule
STIG-ID	WN11-CC-000005
SWIFT-CSCV1	2.3
VULN-ID	V-253350

Assets

lognpacific3286

```
NULL
```

WN11-CC-000007 - Windows 11 must cover or disable the built-in or attached camera when not in use.

Info

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.
Failing to disconnect from collaborative computing devices (i.e. cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnect activity without having to go through complex and tedious procedures.
Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Solution

If the camera is not disconnected or covered, the following registry entry is required.
Registry Hive: HKEY_LOCAL_MACHINE RegistryPath\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam
Value Name: Value Value Data: Deny

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253351r1106508_rule
STIG-ID	WN11-CC-000007
SWIFT-CSCV1	2.3
VULN-ID	V-253351

Assets

lognpacific3286

```
'Allow'
```

WN11-CC-000010 - The display of slide shows on the lock screen must be disabled.

Info

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253352r958478_rule
STIG-ID	WN11-CC-000010
SWIFT-CSCV1	2.3
VULN-ID	V-253352

Assets

lognpacific3286

```
NULL
```

WN11-CC-000020 - IPv6 source routing must be configured to highest protection.

Info

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

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253353r991589_rule
STIG-ID	WN11-CC-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253353

Assets

lognpacific3286

```
NULL
```

WN11-CC-000025 - The system must be configured to prevent IP source routing.

Info

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

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' to 'Highest protection, source routing is completely disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253354r991589_rule
STIG-ID	WN11-CC-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253354

Assets

lognpacific3286

NULL

WN11-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.

Info

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

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' to 'Disabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253355r991589_rule
STIG-ID	WN11-CC-000030
SWIFT-CSCV1	2.3
VULN-ID	V-253355

Assets

lognpacific3286

NULL

WN11-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers.

Info

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 servers WINS resolution capability.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MSS (Legacy) >> 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' to 'Enabled'.
This policy setting requires the installation of the MSS-Legacy custom templates included with the STIG package. 'MSS-Legacy.admx' and 'MSS-Legacy.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-5
800-53R5	SC-5a.
CAT	III
CCI	CCI-002385
CSF	DE.CM-1
CSF	PR.DS-4
CSF2.0	DE.CM-01
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-5
ITSG-33	SC-5a.
NESA	T3.3.1
NIAV2	GS8e
NIAV2	GS10c
QCSC-V1	8.2.1
RULE-ID	SV-253356r958902_rule
STIG-ID	WN11-CC-000035
VULN-ID	V-253356

Assets

lognpacific3286

```
NULL
```

WN11-CC-000038 - WDigest Authentication must be disabled.

Info

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 11. This setting ensures this is enforced.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'WDigest Authentication (disabling may require KB2871997)' to 'Disabled'.
The patch referenced in the policy title is not required for Windows 11.
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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253358r958478_rule
STIG-ID	WN11-CC-000038

SWIFT-CSCV1	2.3
VULN-ID	V-253358

Assets

lognpacific3286

```
NULL
```

WN11-CC-000039 - Run as different user must be removed from context menus.

Info

The 'Run as different user' selection from context menus allows the use of credentials other than the currently logged on user. Using privileged credentials in a standard user session can expose those credentials to theft. Removing this option from context menus helps prevent this from occurring.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Remove 'Run as Different User' from context menus' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253359r958478_rule
STIG-ID	WN11-CC-000039

SWIFT-CSCV1	2.3
VULN-ID	V-253359

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - batfile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - cmdfile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - exefile:
 Remote value: NULL
 Policy value: 4096


-------------------------
FAILED - mscfile:
 Remote value: NULL
 Policy value: 4096
```

WN11-CC-000040 - Insecure logons to an SMB server must be disabled.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253360r991589_rule
STIG-ID	WN11-CC-000040
SWIFT-CSCV1	2.3
VULN-ID	V-253360

Assets

lognpacific3286

```
NULL
```

WN11-CC-000044 - Internet connection sharing must be disabled.

Info

Internet connection sharing makes it possible for an existing internet connection, such as through wireless, to be shared and used by other systems essentially creating a mobile hotspot. This exposes the system sharing the connection to others with potentially malicious purpose.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Connections >> 'Prohibit use of Internet Connection Sharing on your DNS domain network' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253361r958478_rule
STIG-ID	WN11-CC-000044
SWIFT-CSCV1	2.3
VULN-ID	V-253361

Assets

lognpacific3286

```
NULL
```

WN11-CC-000050 - Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.

Info

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

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Network Provider >> 'Hardened UNC Paths' to 'Enabled' with at least the following configured in 'Hardened UNC Paths:' (click the 'Show' button to display).
Value Name: *\SYSVOL Value: RequireMutualAuthentication=1, RequireIntegrity=1
Value Name: *\NETLOGON Value: RequireMutualAuthentication=1, RequireIntegrity=1

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253362r991589_rule
STIG-ID	WN11-CC-000050
SWIFT-CSCV1	2.3
VULN-ID	V-253362

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
```

```
FAILED - SYSVOL:
 Remote value: ''
 Policy value: 'RequireMutualAuthentication=1,[\s]*RequireIntegrity=1'


-------------------------
FAILED - NETLOGON:
 Remote value: ''
 Policy value: 'RequireMutualAuthentication=1,[\s]*RequireIntegrity=1'
```

WN11-CC-000052 - Windows 11 must be configured to prioritize ECC Curves with longer key lengths first.

Info

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. By default Windows uses ECC curves with shorter key lengths first. Requiring ECC curves with longer key lengths to be prioritized first helps ensure more secure algorithms are used.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> SSL Configuration Settings >> 'ECC Curve Order' to 'Enabled' with 'ECC Curve Order:' including the following in the order listed: NistP384 NistP256

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	IA-7
800-53R5	IA-7
CAT	II
CCI	CCI-000803
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
ITSG-33	IA-7
ITSG-33	IA-7a.
NESA	M5.2.1
NESA	M5.2.6
NESA	M5.3.1
NESA	T7.4.1
QCSC-V1	13.2
RULE-ID	SV-253363r971535_rule
STIG-ID	WN11-CC-000052
VULN-ID	V-253363

Assets

lognpacific3286

NULL

WN11-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.

Info

Multiple network connections can provide additional attack vectors to a system and must be limited. When connected to a domain, communication must go through the domain connection.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Windows Connection Manager >> 'Prohibit connection to non-domain networks when connected to domain authenticated network' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253365r991589_rule
STIG-ID	WN11-CC-000060
SWIFT-CSCV1	2.3
VULN-ID	V-253365

Assets

lognpacific3286

```
NULL
```

WN11-CC-000065 - Wi-Fi Sense must be disabled.

Info

Wi-Fi Sense automatically connects the system to known hotspots and networks that contacts have shared. It also allows the sharing of the system's known networks to contacts. Automatically connecting to hotspots and shared networks can expose a system to unsecured or potentially malicious systems.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Network >> WLAN Service >> WLAN Settings>> 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253366r991589_rule
STIG-ID	WN11-CC-000065
SWIFT-CSCV1	2.3
VULN-ID	V-253366

Assets

lognpacific3286

```
NULL
```

WN11-CC-000066 - Command line data must be included in process creation events.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling 'Include command line data for process creation events' will record the command line information with the process creation events in the log. This can provide additional detail when malware has run on a system.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02b.
800-53	AU-3(1)
800-53R5	AU-3(1)
CAT	II
CCI	CCI-000135
CN-L3	7.1.3.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3(1)
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d

NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253367r958422_rule
STIG-ID	WN11-CC-000066
SWIFT-CSCV1	6.4
VULN-ID	V-253367

Assets

lognpacific3286

```
NULL
```

WN11-CC-000068 - Windows 11 must be configured to enable Remote host allows delegation of non-exportable credentials.

Info

An exportable version of credentials is provided to remote hosts when using credential delegation which exposes them to theft on the remote host. Restricted Admin mode or Remote Credential Guard allow delegation of non-exportable credentials providing additional protection of the credentials. Enabling this configures the host to support Restricted Admin mode or Remote Credential Guard.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Credentials Delegation >> 'Remote host allows delegation of non-exportable credentials' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253368r991589_rule
STIG-ID	WN11-CC-000068
SWIFT-CSCV1	2.3
VULN-ID	V-253368

Assets

lognpacific3286

NULL

WN11-CC-000070 - Virtualization-based Security must be enabled on Windows 11 with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.

Info

Virtualization-based Security (VBS) provides the platform for the additional security features, Credential Guard and virtualization-based protection of code integrity. Secure Boot is the minimum security level with DMA protection providing additional memory protection. DMA Protection requires a CPU that supports input/output memory management unit (IOMMU).

Solution

Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Secure Boot' or 'Secure Boot and DMA Protection' selected for 'Select Platform Security Level:'.
A Microsoft article on Credential Guard system requirement can be found at the following link.
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard-requirements

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253369r991589_rule
STIG-ID	WN11-CC-000070
SWIFT-CSCV1	2.3
VULN-ID	V-253369

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - RequiredSecurityProperties:
 Remote value: '0'
 Policy value: '2'


-------------------------
FAILED - VirtualizationBasedSecurityStatus:
 Remote value: '0'
 Policy value: '2'
```

WN11-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.

Info

The default behavior is for Early Launch Antimalware - Boot-Start Driver Initialization policy is to enforce 'Good, unknown and bad but critical' (preventing 'bad'). By being launched first by the kernel, ELAM (Early Launch Antimalware) is ensured to be launched before any third-party software, and is therefore able to detect malware in the boot process and prevent it from initializing.

Solution

Ensure that Early Launch Antimalware - Boot-Start Driver Initialization policy is set to enforce 'Good, unknown and bad but critical' (preventing 'bad').
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Early Launch Antimalware >> 'Boot-Start Driver Initialization Policy' to 'Enabled with 'Good, unknown and bad but critical' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253372r991589_rule
STIG-ID	WN11-CC-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253372

Assets

lognpacific3286

```
NULL
```

WN11-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.

Info

Enabling this setting and then selecting the 'Process even if the Group Policy objects have not changed' option ensures that 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.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Group Policy >> 'Configure registry policy processing' to 'Enabled' and select the option 'Process even if the Group Policy objects have not changed'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253373r991589_rule
STIG-ID	WN11-CC-000090
SWIFT-CSCV1	2.3
VULN-ID	V-253373

Assets

lognpacific3286

```
NULL
```

WN11-CC-000100 - Downloading print driver packages over HTTP must be prevented.

Info

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 uncontrolled updates to the system. This setting prevents the computer from downloading print driver packages over HTTP.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253374r958478_rule
STIG-ID	WN11-CC-000100
SWIFT-CSCV1	2.3

VULN-ID	V-253374

Assets

lognpacific3286

```
NULL
```

WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers.

Info

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 uncontrolled updates to the system. This setting prevents Windows from downloading a list of providers for the Web publishing and online ordering wizards.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> 'Turn off Internet download for Web publishing and online ordering wizards' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253375r958478_rule
STIG-ID	WN11-CC-000105

SWIFT-CSCV1	2.3
VULN-ID	V-253375

Assets

lognpacific3286

```
NULL
```

WN11-CC-000110 - Printing over HTTP must be prevented.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253376r958478_rule
STIG-ID	WN11-CC-000110
SWIFT-CSCV1	2.3

VULN-ID	V-253376

Assets

lognpacific3286

```
NULL
```

WN11-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253378r958478_rule
STIG-ID	WN11-CC-000120
SWIFT-CSCV1	2.3
VULN-ID	V-253378

Assets

lognpacific3286

```
NULL
```

WN11-CC-000145 - Users must be prompted for a password on resume from sleep (on battery).

Info

Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (on battery).

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253380r1051049_rule
STIG-ID	WN11-CC-000145
VULN-ID	V-253380

Assets

lognpacific3286

```
NULL
```

WN11-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in).

Info

Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (plugged in).

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253381r1051050_rule
STIG-ID	WN11-CC-000150
VULN-ID	V-253381

Assets

lognpacific3286

```
NULL
```

WN11-CC-000155 - Solicited Remote Assistance must not be allowed.

Info

Remote assistance allows another user to view or take control of the local session of a user. Solicited assistance is help that is specifically requested by the local user. This may allow unauthorized parties access to the resources on the computer.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Assistance >> 'Configure Solicited Remote Assistance' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253382r958524_rule
STIG-ID	WN11-CC-000155
VULN-ID	V-253382

Assets

lognpacific3286

```
NULL
```

WN11-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server.

Info

Configuring RPC to restrict unauthenticated RPC clients from connecting to the RPC server will prevent anonymous connections.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Procedure Call >> 'Restrict Unauthenticated RPC clients' to 'Enabled' and 'Authenticated'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.02
800-53	IA-3(1)
800-53R5	IA-3(1)
CAT	II
CCI	CCI-001967
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-3(1)
NESA	T5.4.3
QCSC-V1	13.2
RULE-ID	SV-253383r971545_rule
STIG-ID	WN11-CC-000165
TBA-FIISB	27.1
VULN-ID	V-253383

Assets

lognpacific3286

```
NULL
```

WN11-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.

Info

Control of credentials and the system must be maintained within the enterprise. Enabling this setting allows enterprise credentials to be used with modern style apps that support this, instead of Microsoft accounts.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Runtime >> 'Allow Microsoft accounts to be optional' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253384r991589_rule
STIG-ID	WN11-CC-000170
SWIFT-CSCV1	2.3
VULN-ID	V-253384

Assets

lognpacific3286

```
NULL
```

WN11-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253385r958478_rule
STIG-ID	WN11-CC-000175
SWIFT-CSCV1	2.3

VULN-ID	V-253385

Assets

lognpacific3286

```
NULL
```

WN11-CC-000180 - Autoplay must be turned off for non-volume devices.

Info

Allowing autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon as media is inserted in 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).

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253386r958804_rule
STIG-ID	WN11-CC-000180
SWIFT-CSCV1	2.3
VULN-ID	V-253386

Assets

lognpacific3286

```
NULL
```

WN11-CC-000185 - The default autorun behavior must be configured to prevent autorun commands.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253387r958804_rule
STIG-ID	WN11-CC-000185
SWIFT-CSCV1	2.3
VULN-ID	V-253387

Assets

lognpacific3286

```
NULL
```

WN11-CC-000190 - Autoplay must be disabled for all drives.

Info

Allowing autoplay to execute may introduce malicious code to a system. Autoplay begins reading from a drive as soon as media is inserted in 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. If this policy is enabled, autoplay can be disabled on all drives.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> AutoPlay Policies >> 'Turn off AutoPlay' to 'Enabled:All Drives'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.7
800-171R3	03.04.06
800-53	CM-7(2)
800-53R5	CM-7(2)
CAT	I
CCI	CCI-001764
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7(2)
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
QCSC-V1	3.2
RULE-ID	SV-253388r958804_rule
STIG-ID	WN11-CC-000190
SWIFT-CSCV1	2.3
VULN-ID	V-253388

Assets

lognpacific3286

NULL

WN11-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.

Info

Enhanced anti-spoofing provides additional protections when using facial recognition with devices that support it.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Biometrics >> Facial Features >> 'Configure enhanced anti-spoofing' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253389r991589_rule
STIG-ID	WN11-CC-000195
SWIFT-CSCV1	2.3
VULN-ID	V-253389

Assets

lognpacific3286

```
NULL
```

WN11-CC-000197 - Microsoft consumer experiences must be turned off.

Info

Microsoft consumer experiences provides suggestions and notifications to users, which may include the installation of Windows Store apps. Organizations may control the execution of applications through other means such as allowlisting. Turning off Microsoft consumer experiences will help prevent the unwanted installation of suggested applications.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Cloud Content >> 'Turn off Microsoft consumer experiences' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253390r958478_rule
STIG-ID	WN11-CC-000197
SWIFT-CSCV1	2.3

VULN-ID	V-253390

Assets

lognpacific3286

```
NULL
```

WN11-CC-000200 - Administrator accounts must not be enumerated during elevation.

Info

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253391r958518_rule
STIG-ID	WN11-CC-000200
VULN-ID	V-253391

Assets

lognpacific3286

NULL

WN11-CC-000204 - Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.

Info

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 'Enhanced' level for telemetry includes additional information beyond 'Security' and 'Basic' on how Windows and apps are used and advanced reliability data. Windows Analytics can use a 'limited enhanced' level to provide information such as health data for devices.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> 'Limit optional diagnostic data for Windows Analytics' to 'Enabled' with 'Enable Desktop Analytics collection' selected in 'Options:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253392r991589_rule
STIG-ID	WN11-CC-000204
SWIFT-CSCV1	2.3
VULN-ID	V-253392

Assets

lognpacific3286

```
NULL
```

WN11-CC-000205 - Windows Telemetry must not be configured to Full.

Info

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. 'Enhanced' includes additional information on how Windows and apps are used and advanced reliability data. Windows Analytics can use a 'limited enhanced' level to provide information such as health data for devices.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> 'Allow Diagnostic Data' to 'Enabled' with 'Send required diagnostic data' selected in 'Options:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SI-11a.
800-53R5	SI-11a.
CAT	II
CCI	CCI-001312
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-11b.
RULE-ID	SV-253393r958564_rule
STIG-ID	WN11-CC-000205
VULN-ID	V-253393

Assets

lognpacific3286

NULL

WN11-CC-000206 - Windows Update must not obtain updates from other PCs on the internet.

Info

Windows 11 allows Windows Update to obtain updates from additional sources instead of Microsoft. In addition to Microsoft, updates can be obtained from and sent to PCs on the local network as well as on the Internet. This is part of the Windows Update trusted process, however to minimize outside exposure, obtaining updates from or sending to systems on the internet must be prevented.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Delivery Optimization >> 'Download Mode' to 'Enabled' with any option except 'Internet' selected.
Acceptable selections include:
Bypass (100) Group (2) HTTP only (0) LAN (1) Simple (99)
.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253394r991589_rule
STIG-ID	WN11-CC-000206
SWIFT-CSCV1	2.3
VULN-ID	V-253394

Assets

lognpacific3286

NULL

WN11-CC-000210 - The Microsoft Defender SmartScreen for Explorer must be enabled.

Info

Microsoft Defender SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling Microsoft Defender SmartScreen will warn or prevent users from running potentially malicious programs.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Configure Windows Defender SmartScreen' to 'Enabled' with 'Warn and prevent bypass' selected. Windows 11 includes duplicate policies for this setting. It can also be configured under Computer Configuration >> Administrative Templates >> Windows Components >> Windows Defender SmartScreen >> Explorer.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253395r958478_rule
STIG-ID	WN11-CC-000210
SWIFT-CSCV1	2.3

VULN-ID V-253395

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - EnableSmartScreen:
 Remote value: NULL
 Policy value: 1


-------------------------
FAILED - ShellSmartScreenLevel:
 Remote value: ''
 Policy value: 'Block'
```

WN11-CC-000252 - Windows 11 must be configured to disable Windows Game Recording and Broadcasting.

Info

Windows Game Recording and Broadcasting is intended for use with games; however, it could potentially record screen shots of other applications and expose sensitive data. Disabling the feature will prevent this from occurring.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Game Recording and Broadcasting >> 'Enables or disables Windows Game Recording and Broadcasting' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253399r958478_rule
STIG-ID	WN11-CC-000252
SWIFT-CSCV1	2.3

VULN-ID	V-253399

Assets

lognpacific3286

NULL

WN11-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled.

Info

The use of a Trusted Platform Module (TPM) to store keys for Windows Hello for Business provides additional security. Keys stored in the TPM may only be used on that system while keys stored using software are more susceptible to compromise and could be used on other systems.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Hello for Business >> 'Use a hardware security device' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253400r991589_rule
STIG-ID	WN11-CC-000255
SWIFT-CSCV1	2.3
VULN-ID	V-253400

Assets

lognpacific3286

NULL

WN11-CC-000260 - Windows 11 must be configured to require a minimum pin length of six characters or greater.

Info

Windows allows the use of PINs as well as biometrics for authentication without sending a password to a network or website where it could be compromised. Longer minimum PIN lengths increase the available combinations an attacker would have to attempt. Shorter minimum length significantly reduces the strength.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> PIN Complexity >> 'Minimum PIN length' to '6' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253401r991589_rule
STIG-ID	WN11-CC-000260
SWIFT-CSCV1	2.3
VULN-ID	V-253401

Assets

lognpacific3286

NULL

WN11-CC-000270 - Passwords must not be saved in the Remote Desktop Client.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253402r1051051_rule
STIG-ID	WN11-CC-000270
VULN-ID	V-253402

Assets

lognpacific3286

```
NULL
```

WN11-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.

Info

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

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	II
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253403r958524_rule
STIG-ID	WN11-CC-000275
VULN-ID	V-253403

Assets

lognpacific3286

```
NULL
```

WN11-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253404r1051052_rule
STIG-ID	WN11-CC-000280
VULN-ID	V-253404

Assets

lognpacific3286

NULL

WN11-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.13
800-171R3	03.13.08
800-53	AC-17(2)
800-53R5	AC-17(2)
CAT	II
CCI	CCI-001453
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.4.1(c)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.6.7
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(2)
NESA	T5.4.2
NIAV2	AM37
PCI-DSSV3.2.1	2.3

PCI-DSSV4.0	2.2.7
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
RULE-ID	SV-253405r991554_rule
STIG-ID	WN11-CC-000285
SWIFT-CSCV1	2.6
VULN-ID	V-253405

Assets

lognpacific3286

NULL

WN11-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level.

Info

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.

Solution

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' and 'High Level'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.13
800-171R3	03.13.08
800-53	AC-17(2)
800-53R5	AC-17(2)
CAT	II
CCI	CCI-000068
CN-L3	7.1.2.7(g)
CN-L3	7.1.3.1(d)
CN-L3	8.1.4.1(c)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.14
ISO-27001-2022	A.6.7
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(2)
NESA	T5.4.2
NIAV2	AM37
PCI-DSSV3.2.1	2.3

PCI-DSSV4.0	2.2.7
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
RULE-ID	SV-253406r958408_rule
STIG-ID	WN11-CC-000290
SWIFT-CSCV1	2.6
VULN-ID	V-253406

Assets

lognpacific3286

NULL

WN11-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253407r991589_rule
STIG-ID	WN11-CC-000295
SWIFT-CSCV1	2.3
VULN-ID	V-253407

Assets

lognpacific3286

```
NULL
```

WN11-CC-000305 - Indexing of encrypted files must be turned off.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253409r958478_rule
STIG-ID	WN11-CC-000305
SWIFT-CSCV1	2.3
VULN-ID	V-253409

Assets

lognpacific3286

```
NULL
```

WN11-CC-000310 - Users must be prevented from changing installation options.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.9
800-53	CM-11(2)
800-53R5	CM-11(2)
CAT	II
CCI	CCI-001812
CCI	CCI-003980
CSF	DE.CM-3
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.6.2
QCSC-V1	8.2.1
RULE-ID	SV-253410r1051053_rule
STIG-ID	WN11-CC-000310
SWIFT-CSCV1	5.1
VULN-ID	V-253410

Assets

lognpacific3286

NULL

WN11-CC-000315 - The Windows Installer feature 'Always install with elevated privileges' must be disabled.

Info

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.9
800-53	CM-11(2)
800-53R5	CM-11(2)
CAT	I
CCI	CCI-001812
CCI	CCI-003980
CSF	DE.CM-3
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
CSF2.0	PR.PS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.6.2
QCSC-V1	8.2.1
RULE-ID	SV-253411r1051054_rule
STIG-ID	WN11-CC-000315
SWIFT-CSCV1	5.1
VULN-ID	V-253411

Assets

lognpacific3286

NULL

WN11-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253413r991591_rule
STIG-ID	WN11-CC-000325
SWIFT-CSCV1	2.3
VULN-ID	V-253413

Assets

lognpacific3286

NULL

WN11-CC-000326 - PowerShell script block logging must be enabled on Windows 11.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling PowerShell script block logging will record detailed information from the processing of PowerShell commands and scripts. This can provide additional detail when malware has run on a system.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02b.
800-53	AU-3(1)
800-53R5	AU-3(1)
CAT	II
CCI	CCI-000135
CN-L3	7.1.3.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3(1)
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d

NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253414r958422_rule
STIG-ID	WN11-CC-000326
SWIFT-CSCV1	6.4
VULN-ID	V-253414

Assets

lognpacific3286

```
NULL
```

WN11-CC-000327 - PowerShell Transcription must be enabled on Windows 11.

Info

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.
Enabling PowerShell Transcription will record detailed information from the processing of PowerShell commands and scripts. This can provide additional detail when malware has run on a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> 'Turn on PowerShell Transcription' to 'Enabled'.
Specify the Transcript output directory to point to a Central Log Server or another secure location to prevent user access.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.02a.
800-53	AU-3
800-53R5	AU-3e.
CAT	II
CCI	CCI-000134
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSF	PR.PT-1
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.28
ISO-27001-2022	A.8.15
ITSG-33	AU-3
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
PCI-DSSV3.2.1	10.3
PCI-DSSV3.2.1	10.3.1
PCI-DSSV3.2.1	10.3.2
PCI-DSSV3.2.1	10.3.3
PCI-DSSV3.2.1	10.3.4
PCI-DSSV3.2.1	10.3.5
PCI-DSSV3.2.1	10.3.6
PCI-DSSV4.0	10.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253415r958420_rule
STIG-ID	WN11-CC-000327
SWIFT-CSCV1	6.4
VULN-ID	V-253415

Assets

lognpacific3286

```
NULL
```

WN11-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	I
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253416r958510_rule
STIG-ID	WN11-CC-000330
TBA-FIISB	45.2.3
VULN-ID	V-253416

Assets

lognpacific3286

NULL

WN11-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05
800-53	MA-4(6)
800-53R5	MA-4(6)
CAT	II
CCI	CCI-002890
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4(6)
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253417r958848_rule
STIG-ID	WN11-CC-000335
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-253417

Assets

lognpacific3286

```
NULL
```

WN11-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> 'Allow Basic authentication' to 'Disabled'.
Severity Override Guidance: The AO can allow the severity override if they have reviewed the overall protection. This would only be allowed temporarily for implementation as documented and approved.
....
Allowing Basic authentication to be used for the sole creation of Office 365 DoD tenants.
....
A documented mechanism and or script that can disable Basic authentication once administration completes.
....
Use of a Privileged Access Workstation (PAW) and adherence to the Clean Source principle for administration.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	I
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253418r958510_rule
STIG-ID	WN11-CC-000345
TBA-FIISB	45.2.3
VULN-ID	V-253418

Assets

lognpacific3286

```
NULL
```

WN11-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05
800-53	MA-4(6)
800-53R5	MA-4(6)
CAT	II
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4(6)
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253419r958850_rule
STIG-ID	WN11-CC-000350
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-253419

Assets

lognpacific3286

```
NULL
```

WN11-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253420r1051055_rule
STIG-ID	WN11-CC-000355
VULN-ID	V-253420

Assets

lognpacific3286

NULL

WN11-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.7.5
800-171R3	03.07.05b.
800-53	MA-4c.
800-53R5	MA-4c.
CAT	II
CCI	CCI-000877
CSF	PR.MA-2
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	MA-4c.
NESA	T2.3.4
NESA	T5.4.4
QCSC-V1	5.2.2
RULE-ID	SV-253421r958510_rule
STIG-ID	WN11-CC-000360
TBA-FIISB	45.2.3
VULN-ID	V-253421

Assets

lognpacific3286

NULL

WN11-CC-000365 - Windows 11 must be configured to prevent Windows apps from being activated by voice while the system is locked.

Info

Allowing Windows apps to be activated by voice from the lock screen could allow for unauthorized use. Requiring logon will ensure the apps are only used by authorized personnel.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Privacy >> 'Let Windows apps activate with voice while the system is locked' to 'Enabled' with Default for all Apps: set to Force Deny.
The requirement is NA if the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> App Privacy >> 'Let Windows apps activate with voice' is configured to 'Enabled' with Default for all Apps: set to Force Deny.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10b.
800-53	AC-11b.
800-53R5	AC-11b.
CAT	II
CCI	CCI-000056
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11b.
NIAV2	AM23e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-253422r958400_rule
STIG-ID	WN11-CC-000365
VULN-ID	V-253422

Assets

lognpacific3286

```
NULL
```

WN11-CC-000370 - The convenience PIN for Windows 11 must be disabled.

Info

This policy controls whether a domain user can sign in using a convenience PIN to prevent enabling (Password Stuffer).

Solution

Disable the convenience PIN sign-in.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> Set 'Turn on convenience PIN sign-in' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253423r958478_rule
STIG-ID	WN11-CC-000370
SWIFT-CSCV1	2.3
VULN-ID	V-253423

Assets

lognpacific3286

```
NULL
```

WN11-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock.

Info

This action secures Windows Ink, which contains applications and features oriented toward pen computing.

Solution

Disable the convenience PIN sign-in.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Ink Workspace >> Set 'Allow Windows Ink Workspace' to 'Enabled and set Options 'On, but disallow access above lock'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10
800-53	AC-11(1)
800-53R5	AC-11(1)
CAT	II
CCI	CCI-000060
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.7.7
ISO-27001-2022	A.8.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11(1)
NIAV2	AM23c
NIAV2	AM23d
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-253424r958404_rule
STIG-ID	WN11-CC-000385
VULN-ID	V-253424

Assets

lognpacific3286

```
NULL
```

WN11-CC-000390 - Windows 11 must be configured to prevent users from receiving suggestions for third-party or additional applications.

Info

Windows spotlight features may suggest apps and content from third-party software publishers in addition to Microsoft apps and content.

Solution

Configure the policy value for User Configuration >> Administrative Templates. >> Windows Components >> Cloud Content >> 'Do not suggest third-party content in Windows spotlight' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253425r958478_rule
STIG-ID	WN11-CC-000390
SWIFT-CSCV1	2.3
VULN-ID	V-253425

Assets

lognpacific3286

```
Non-compliant items:
  HKU\S-1-5-21-108538807-2850267539-2289239689-500\Software\Policies\Microsoft\Windows
\CloudContent -
```

WN11-CC-000391 - Internet Explorer must be disabled for Windows 11.

Info

Internet Explorer 11 (IE11) is not supported on Windows 11 semi-annual channel.

Solution

For Windows 11 semi-annual channel, remove or disable the IE11 application.
To disable IE11 as a standalone browser:
Set the policy value for 'Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser' to 'Enabled' with the option value set to 'Never'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-256893r958552_rule
STIG-ID	WN11-CC-000391
SWIFT-CSCV1	2.3
VULN-ID	V-256893

Assets

lognpacific3286

```
NULL
```

WN11-EP-000310 - Windows 11 Kernel (Direct Memory Access) DMA Protection must be enabled.

Info

Kernel DMA Protection to protect PCs against drive-by Direct Memory Access (DMA) attacks using PCI hot plug devices connected to Thunderbolt 3 ports. Drive-by DMA attacks can lead to disclosure of sensitive information residing on a PC, or even injection of malware that allows attackers to bypass the lock screen or control PCs remotely.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Kernel DMA Protection >> 'Enumeration policy for external devices incompatible with Kernel DMA Protection' to 'Enabled' with 'Enumeration Policy' set to 'Block All'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253426r991580_rule
STIG-ID	WN11-EP-000310
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253426

Assets

lognpacific3286

NULL

WN11-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store.

Info

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.

Solution

Install the DoD Root CA certificates.
DoD Root CA 3 DoD Root CA 4 DoD Root CA 5 DoD Root CA 6
The InstallRoot tool is available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.12
800-53	IA-5(2)(a)
800-53R5	IA-5(2)(b)(1)
CAT	II
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(2)(a)
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253427r958448_rule
STIG-ID	WN11-PK-000005
VULN-ID	V-253427

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 4:
 Remote value: 'No matching certificates found'
 Policy value: 'B8269F25DBD937ECAFD4C35A9838571723F2D026'


-------------------------
FAILED - Root CA 6:
 Remote value: 'No matching certificates found'
 Policy value: 'D37ECF61C0B4ED88681EF3630C4E2FC787B37AEF'


-------------------------
FAILED - Root CA 5:
 Remote value: 'No matching certificates found'
 Policy value: '4ECB5CC3095670454DA1CBD410FC921F46B8564B'


-------------------------
FAILED - Root CA 3:
 Remote value: 'No matching certificates found'
 Policy value: 'D73CA91102A2204A36459ED32213B467D7CE97FB'
```

WN11-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.

Info

To ensure secure websites protected with External Certificate Authority (ECA) server certificates are properly validated, the system must trust the ECA Root CAs. The ECA root certificates will ensure the trust chain is established for server certificates issued from the External CAs. This requirement only applies to unclassified systems.

Solution

Install the ECA Root CA certificates on unclassified systems.
ECA Root CA 4
The InstallRoot tool is available on Cyber Exchange at https://cyber.mil/pki-pke/tools-configuration-files. PKI can be found at https://crl.gds.disa.mil/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.12
800-53	IA-5(2)(a)
800-53R5	IA-5(2)(b)(1)
CAT	II
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(2)(a)
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253428r958448_rule
STIG-ID	WN11-PK-000010

VULN-ID	V-253428

Assets

lognpacific3286

```
'No matching certificates found'
```

WN11-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Info

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.

Solution

Install the DoD Interoperability Root CA cross-certificates on unclassified systems.
Issued To - Issued By - Thumbprint DoD Root CA 3 - DoD Interoperability Root CA 2 - 49CBE933151872E17C8EAE7F0ABA97FB610F6477
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/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.15
800-171R3	03.13.15
800-53	SC-23(5)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-002470
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
QCSC-V1	5.2.1
RULE-ID	SV-253429r958448_rule
STIG-ID	WN11-PK-000015
VULN-ID	V-253429

Assets

lognpacific3286

```
'No matching certificates found'
```

WN11-PK-000020 - The US DOD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.

Info

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.

Solution

Install the US DOD CCEB Interoperability Root CA cross-certificate on unclassified systems.
Issued To - Issued By - Thumbprint 9B74964506C7ED9138070D08D5F8B969866560C8 NotAfter: 7/18/2025 9:56:22 AM Issued To: DOD Root CA 6 Issued By: US DOD CCEB Interoperability Root CA 2 Thumbprint: D471CA32F7A692CE6CBB6196BD3377FE4DBCD106 NotAfter: 7/18/2026
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/.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.15
800-171R3	03.13.15
800-53	SC-23(5)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-002470
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
QCSC-V1	5.2.1
RULE-ID	SV-253430r1081058_rule
STIG-ID	WN11-PK-000020
VULN-ID	V-253430

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Root CA 3:
 Remote value: 'No matching certificates found'
 Policy value: '[a-zA-Z\s-]*CN=DoD Root CA 3, OU=PKI, OU=DoD, O=U\.S\. Government, C=US'
```

```
-------------------------
FAILED - Root CA 6:
 Remote value: 'No matching certificates found'
 Policy value: '[a-zA-Z\s-]*CN=DoD Root CA 6, OU=PKI, OU=DoD, O=U\.S\. Government, C=US'
```

WN11-SO-000005 - The built-in administrator account must be disabled.

Info

The built-in administrator account is a well-known account subject to attack. It also provides no accountability to individual administrators on a system. It must be disabled to prevent its use.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Administrator account status' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.1
800-171R3	03.05.01a.
800-53	IA-2
800-53R5	IA-2
CAT	II
CCI	CCI-000764
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-2
ITSG-33	IA-2a.
NESA	T2.3.8
NESA	T5.3.1

NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253432r958482_rule
STIG-ID	WN11-SO-000005
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-253432

Assets

lognpacific3286

```
'enabled'
```

WN11-SO-000010 - The built-in guest account must be disabled.

Info

A system faces an increased vulnerability threat if the built-in guest account is not disabled. This account is a known account that exists on all Windows systems and cannot be deleted. This account is initialized during the installation of the operating system with no password assigned.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Accounts: Guest account status' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	IA-8
800-53R5	IA-8
CAT	II
CCI	CCI-000804
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-8
ITSG-33	IA-8a.
NESA	T4.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253433r958504_rule
STIG-ID	WN11-SO-000010
SWIFT-CSCV1	2.8

VULN-ID	V-253433

Assets

lognpacific3286

```
'enabled'
```

WN11-SO-000025 - The built-in guest account must be renamed.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253436r991589_rule
STIG-ID	WN11-SO-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253436

Assets

lognpacific3286

```
'Guest'
```

WN11-SO-000030 - Audit policy using subcategories must be enabled.

Info

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

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12a.
800-53R5	AU-12a.
CAT	II
CCI	CCI-000169
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-12a.
PCI-DSSV3.2.1	10.1

QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253437r958442_rule
STIG-ID	WN11-SO-000030
SWIFT-CSCV1	6.4
VULN-ID	V-253437

Assets

lognpacific3286

NULL

WN11-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.

Info

Unattended systems are susceptible to unauthorized use and must be locked when unattended. The screen saver must 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.
Satisfies: SRG-OS-000279-GPOS-00109, SRG-OS-000163-GPOS-00072

Solution

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.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.11
800-171	3.13.9
800-171R3	03.01.11
800-171R3	03.13.09
800-53	AC-12
800-53	SC-10
800-53R5	AC-12
800-53R5	SC-10
CAT	II
CCI	CCI-001133
CCI	CCI-002361
CN-L3	7.1.2.2(d)
CN-L3	7.1.3.7(b)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO-27001-2022	A.8.20
ITSG-33	AC-12
ITSG-33	SC-10

ITSG-33	SC-10a.
NESA	T2.3.8
NESA	T4.5.1
NESA	T5.5.1
NIAV2	NS49
RULE-ID	SV-253444r958636_rule
STIG-ID	WN11-SO-000070
SWIFT-CSCV1	2.6
VULN-ID	V-253444

Assets

lognpacific3286

```
NULL
```

WN11-SO-000075 - The required legal notice must be configured to display before console logon.

Info

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.
Satisfies: SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088, SRG-OS-000024-GPOS-00007

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Message text for users attempting to log on' to the following.
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.8
800-171	3.1.9
800-171R3	03.01.08a.
800-171R3	03.01.09
800-53	AC-7a.
800-53	AC-8a.
800-53	AC-8b.
800-53R5	AC-7a.
800-53R5	AC-8a.
800-53R5	AC-8b.
CAT	II
CCI	CCI-000044
CCI	CCI-000048
CCI	CCI-000050
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
ITSG-33	AC-8a.
ITSG-33	AC-8b.
NESA	M5.2.5
NESA	T5.5.1
NIAV2	AM10a
NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
NIAV2	AM10f
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
RULE-ID	SV-253445r958392_rule
STIG-ID	WN11-SO-000075
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
TBA-FIISB	45.2.4
VULN-ID	V-253445

Assets

lognpacific3286

```
'No content provided to compare with.'
```

WN11-SO-000080 - The Windows message title for the legal notice must be configured.

Info

Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Message title for users attempting to log on' to 'DoD Notice and Consent Banner', 'US Department of Defense Warning Statement', or a site-defined equivalent.
If a site-defined title is used, it can in no case contravene or modify the language of the banner text required in WN11-SO-000075.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8a.
800-53	AC-8c.1.
800-53	AC-8c.2.
800-53	AC-8c.3.
800-53R5	AC-8a.
800-53R5	AC-8c.1.
800-53R5	AC-8c.2.
800-53R5	AC-8c.3.
CAT	III
CCI	CCI-000048
CCI	CCI-001384
CCI	CCI-001385
CCI	CCI-001386
CCI	CCI-001387
CCI	CCI-001388
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8a.
ITSG-33	AC-8c.a.

ITSG-33	AC-8c.b.
ITSG-33	AC-8c.c.
NESA	M5.2.5
NESA	T5.5.1
NIAV2	AM10a
NIAV2	AM10b
NIAV2	AM10c
NIAV2	AM10d
NIAV2	AM10e
RULE-ID	SV-253446r958586_rule
STIG-ID	WN11-SO-000080
TBA-FIISB	45.2.4
VULN-ID	V-253446

Assets

lognpacific3286

```
'No content provided to compare with.'
```

WN11-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253448r991589_rule
STIG-ID	WN11-SO-000095
SWIFT-CSCV1	2.3
VULN-ID	V-253448

Assets

lognpacific3286

```
'0'
```

WN11-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing.

Info

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.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10

ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253449r958908_rule
STIG-ID	WN11-SO-000100
VULN-ID	V-253449

Assets

lognpacific3286

NULL

WN11-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.

Info

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.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10

ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253451r958908_rule
STIG-ID	WN11-SO-000120
VULN-ID	V-253451

Assets

lognpacific3286

NULL

WN11-SO-000150 - Anonymous enumeration of shares must be restricted.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253454r958524_rule
STIG-ID	WN11-SO-000150
VULN-ID	V-253454

Assets

lognpacific3286

0

WN11-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.

Info

The Windows SAM stores users' passwords. Restricting remote rpc connections to the SAM to Administrators helps protect those credentials.

Solution

Navigate to the policy Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Restrict clients allowed to make remote calls to SAM'.
Select 'Edit Security' to configure the 'Security descriptor:'.
Add 'Administrators' in 'Group or user names:' if it is not already listed (this is the default).
Select 'Administrators' in 'Group or user names:'.
Select 'Allow' for 'Remote Access' in 'Permissions for 'Administrators'.
Click 'OK'.
The 'Security descriptor:' must be populated with 'O:BAG:BAD:(A;;RC;;;BA) for the policy to be enforced.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1

NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253457r1081060_rule
STIG-ID	WN11-SO-000167
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253457

Assets

lognpacific3286

' '

WN11-SO-000180 - NTLM must be prevented from falling back to a Null session.

Info

NTLM sessions that are allowed to fall back to Null (unauthenticated) sessions may gain unauthorized access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253458r991589_rule
STIG-ID	WN11-SO-000180
SWIFT-CSCV1	2.3
VULN-ID	V-253458

Assets

lognpacific3286

```
NULL
```

WN11-SO-000185 - PKU2U authentication using online identities must be prevented.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253459r991589_rule
STIG-ID	WN11-SO-000185
SWIFT-CSCV1	2.3
VULN-ID	V-253459

Assets

lognpacific3286

```
NULL
```

WN11-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.

Info

Certain encryption types are no longer considered secure. This setting configures a minimum encryption type for Kerberos, preventing the use of the DES and RC4 encryption suites.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Configure encryption types allowed for Kerberos' to 'Enabled' with only the following selected:
AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	IA-7
800-53R5	IA-7
CAT	II
CCI	CCI-000803
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
ITSG-33	IA-7
ITSG-33	IA-7a.
NESA	M5.2.1
NESA	M5.2.6
NESA	M5.3.1
NESA	T7.4.1
QCSC-V1	13.2
RULE-ID	SV-253460r971535_rule
STIG-ID	WN11-SO-000190
VULN-ID	V-253460

Assets

lognpacific3286

NULL

WN11-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.

Info

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 stand-alone computers that are running later versions.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253462r991589_rule
STIG-ID	WN11-SO-000205
SWIFT-CSCV1	2.3
VULN-ID	V-253462

Assets

lognpacific3286

NULL

WN11-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.

Info

Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.

Solution

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).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253464r991589_rule
STIG-ID	WN11-SO-000215
SWIFT-CSCV1	2.3
VULN-ID	V-253464

Assets

lognpacific3286

536870912

WN11-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.

Info

Microsoft has implemented a variety of security support providers for use with RPC sessions. All of the options must be enabled to ensure the maximum security level.

Solution

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).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253465r991589_rule
STIG-ID	WN11-SO-000220
SWIFT-CSCV1	2.3
VULN-ID	V-253465

Assets

lognpacific3286

536870912

WN11-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

Info

This setting ensures that 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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.11
800-171R3	03.13.11
800-53	SC-13
800-53R5	SC-13b.
CAT	II
CCI	CCI-002450
CSF	PR.DS-5
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.8.24
ISO/IEC-27001	A.10.1.1
ITSG-33	SC-13
ITSG-33	SC-13a.
NESA	M5.2.6
NESA	T7.4.1
NIAV2	CY3

NIAV2	CY4
NIAV2	CY5b
NIAV2	CY5c
NIAV2	CY5d
NIAV2	CY7
NIAV2	NS5e
QCSC-V1	6.2
RULE-ID	SV-253466r959006_rule
STIG-ID	WN11-SO-000230
VULN-ID	V-253466

Assets

lognpacific3286

```
0
```

WN11-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253468r1051057_rule
STIG-ID	WN11-SO-000245
VULN-ID	V-253468

Assets

lognpacific3286

```
NULL
```

WN11-SO-000250 - User Account Control must prompt administrators for consent on the secure desktop.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253469r958518_rule
STIG-ID	WN11-SO-000250
VULN-ID	V-253469

Assets

lognpacific3286

5

WN11-SO-000255 - User Account Control must automatically deny elevation requests for standard users.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. Denying elevation requests from standard user accounts requires tasks that need elevation to be initiated by accounts with administrative privileges. This ensures correct accounts are used on the system for privileged tasks to help mitigate credential theft.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253471r1051058_rule
STIG-ID	WN11-SO-000255
VULN-ID	V-253471

Assets

lognpacific3286

3

WN11-SO-000280 - Passwords for enabled local Administrator accounts must be changed at least every 60 days.

Info

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the password. A local Administrator account is not generally used and its password may not be changed as frequently as necessary. Changing the password for enabled Administrator accounts on a regular basis will limit its exposure. Windows LAPS must be used to change the built-in Administrator account password.

Solution

Change the enabled local Administrator account password at least every 60 days.
Windows LAPS must be used to change the built-in Administrator account password. Domain-joined and nondomain-joined systems can configure this to occur more frequently. LAPS will change the password every 30 days by default. More information is available at:
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/by-popular-demand-windows-laps-available-now/ba-p/3788747 https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview#windows-laps-supported-platforms-and-azure-ad-laps-preview-status

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3

ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253476r1051060_rule
STIG-ID	WN11-SO-000280
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253476

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Password last set date for Admin account.:
 Remote value: 'PASS: Password age within recommended limits'
 Policy value: 'PASS: Password age within recommended limits'


-------------------------
FAILED - LAPS password age configured.:
 Remote value: NULL
 Policy value: [0..60]


-------------------------
FAILED - LAPS password length configured.:
 Remote value: NULL
 Policy value: [14..4294967295]


-------------------------
FAILED - LAPS password complexity configured.:
 Remote value: NULL
 Policy value: 4


-------------------------
FAILED - LAPS name of administrator account enabled.:
 Remote value: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies
\LAPS_registry_does_not_exist'
 Policy value: 'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS'
```

WN11-UC-000015 - Toast notifications to the lock screen must be turned off.

Info

Toast notifications 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.

Solution

Configure the policy value for User Configuration >> Administrative Templates >> Start Menu and Taskbar >> Notifications >> 'Turn off toast notifications on the lock screen' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	III
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253477r958478_rule
STIG-ID	WN11-UC-000015
SWIFT-CSCV1	2.3
VULN-ID	V-253477

Assets

lognpacific3286

```
Non-compliant items:
  HKU\S-1-5-21-108538807-2850267539-2289239689-500\Software\Policies\Microsoft\Windows
\CurrentVersion\PushNotifications -
```

WN11-UR-000010 - The 'Access this computer from the network' user right must only be assigned to the Administrators and Remote Desktop Users groups.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Access this computer from the network' user right may access resources on the system, and must be limited to those that require it.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Access this computer from the network' to only include the following groups or accounts: Administrators Remote Desktop Users

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3

ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253480r958472_rule
STIG-ID	WN11-UR-000010
TBA-FIISB	31.1
VULN-ID	V-253480

Assets

lognpacific3286

```
'backup operators' && 'users' && 'administrators' && 'everyone'
```

WN11-UR-000025 - The 'Allow log on locally' user right must only be assigned to the Administrators and Users groups.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Allow log on locally' user right can log on interactively to a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Allow log on locally' to only include the following groups or accounts:
Administrators Users

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3

ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253482r958472_rule
STIG-ID	WN11-UR-000025
TBA-FIISB	31.1
VULN-ID	V-253482

Assets

lognpacific3286

```
'backup operators' && 'users' && 'administrators' && 'guest'
```

WN11-UR-000030 - The 'Back up files and directories' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Back up files and directories' user right can circumvent file and directory permissions and could allow access to sensitive data.'

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Back up files and directories' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253483r958726_rule
STIG-ID	WN11-UR-000030
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253483

Assets

lognpacific3286

```
'backup operators' && 'administrators'
```

WN11-UR-000070 - The 'Deny access to this computer from the network' user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny access to this computer from the network' right defines the accounts that are prevented from logging on from the network.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny access to this computer from the network' to include the following:
Domain Systems Only:
Enterprise Admins group Domain Admins group Local account (see Note below)
All Systems:
Guests group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
Note: 'Local account' is a built-in security group used to assign user rights and permissions to all local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253491r958472_rule
STIG-ID	WN11-UR-000070
TBA-FIISB	31.1
VULN-ID	V-253491

Assets

lognpacific3286

```
'guest'
```

WN11-UR-000085 - The 'Deny log on locally' user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on locally' right defines accounts that are prevented from logging on interactively.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on locally' to include the following:
Domain Systems Only:
Enterprise Admins Group Domain Admins Group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
All Systems:
Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253494r958472_rule
STIG-ID	WN11-UR-000085
TBA-FIISB	31.1
VULN-ID	V-253494

Assets

lognpacific3286

```
'guest'
```

WN11-UR-000090 - The 'Deny log on through Remote Desktop Services' user right on Windows 11 workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on through Remote Desktop Services' right defines the accounts that are prevented from logging on using Remote Desktop Services.
If Remote Desktop Services is not used by the organization, the Everyone group must be assigned this right to prevent all access.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.
Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.
The Guests group must be assigned this right to prevent unauthenticated access.

Solution

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:
If Remote Desktop Services is not used by the organization, assign the Everyone group this right to prevent all access.
Domain Systems Only:
Enterprise Admins group Domain Admins group Local account (see Note below)
All Systems:
Guests group
Privileged Access Workstations (PAWs) dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. (See the Windows Privileged Access Workstation STIG for PAW requirements.)
Note: 'Local account' is a built-in security group used to assign user rights and permissions to all local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171	3.1.12
800-171R3	03.01.02
800-171R3	03.01.12
800-53	AC-3
800-53	AC-17(1)
800-53R5	AC-3
800-53R5	AC-17(1)
CAT	II
CCI	CCI-000213
CCI	CCI-002314
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.4(c)
CN-L3	8.1.4.11(b)

CN-L3	8.1.10.2(c)
CN-L3	8.1.10.6(i)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-3
CSF	PR.AC-4
CSF	PR.PT-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.16
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
ITSG-33	AC-17(1)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1

NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253495r958472_rule
STIG-ID	WN11-UR-000090
SWIFT-CSCV1	2.6
TBA-FIISB	31.1
VULN-ID	V-253495

Assets

lognpacific3286

NULL

WN11-UR-000110 - The 'Impersonate a client after authentication' user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Impersonate a client after authentication' user right allows a program to impersonate another user or account to run on their behalf. An attacker could potentially use this to elevate privileges.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Impersonate a client after authentication' to only include the following groups or accounts: Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253498r958726_rule
STIG-ID	WN11-UR-000110
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253498

Assets

lognpacific3286

```
'printspoolerservice' && 'service' && 'administrators' && 'network service' && 'local service'
```

WN11-UR-000160 - The 'Restore files and directories' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Restore files and directories' user right can circumvent file and directory permissions and could allow access to sensitive data. It could also be used to over-write more current data.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Restore files and directories' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253505r958726_rule
STIG-ID	WN11-UR-000160
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253505

Assets

lognpacific3286

```
'backup operators' && 'administrators'
```

Audits SKIPPED

Audits PASSED

DISA_Microsoft_Windows_11_STIG_v2r4.audit from DISA Microsoft Windows 11 STIG v2r4

Info

Solution

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Windows 11 is installed:
 Remote value: '26100'
 Policy value: '2[26][0-9]{3}'


-------------------------
PASSED - Windows 11 installation type:
 Remote value: 'Client'
 Policy value: 'Client'
```

WN11-00-000005 - Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version.

Info

Features such as Credential Guard use virtualization-based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization-based security and Credential Guard are only available with Windows 11 Enterprise 64-bit version.

Solution

Use Windows 11 Enterprise 64-bit version for domain-joined systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253254r991589_rule
STIG-ID	WN11-00-000005
SWIFT-CSCV1	2.3
VULN-ID	V-253254

Assets

lognpacific3286

PASSED

WN11-00-000010 - Windows 11 domain-joined systems must have a Trusted Platform Module (TPM) enabled.

Info

Credential Guard uses virtualization-based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Without a TPM enabled and ready for use, Credential Guard keys are stored in a less secure method using software.

Solution

For standalone systems, this is NA.
Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Ensure domain-joined systems must have a TPM that is configured for use. (Versions 2.0 support Credential Guard.)
The TPM must be enabled in the firmware.
Run 'tpm.msc' for configuration options in Windows.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253255r971547_rule
STIG-ID	WN11-00-000010
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253255

Assets

lognpacific3286

PASSED

WN11-00-000015 - Windows 11 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.

Info

UEFI provides additional security features in comparison to legacy BIOS firmware, including Secure Boot. UEFI is required to support additional security features in Windows 11, including virtualization-based Security and Credential Guard. Systems with UEFI that are operating in Legacy BIOS mode will not support these security features.

Solution

Configure UEFI firmware to run in UEFI mode, not Legacy BIOS mode.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253256r971547_rule
STIG-ID	WN11-00-000015
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253256

Assets

lognpacific3286

```
'path                    \Windows\system32\winload.efi'
```

WN11-00-000020 - Secure Boot must be enabled on Windows 11 systems.

Info

Secure Boot is a standard that ensures systems boot only to a trusted operating system. Secure Boot is required to support additional security features in Windows 11, including virtualization-based Security and Credential Guard. If Secure Boot is turned off, these security features will not function.

Solution

Enable Secure Boot in the system firmware.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(1)
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8(1)
NESA	T7.4.1
NIAV2	NS5d
NIAV2	NS6b
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253257r971547_rule
STIG-ID	WN11-00-000020
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253257

Assets

lognpacific3286

```
'True'
```

WN11-00-000040 - Windows 11 systems must be maintained at a supported servicing level.

Info

Windows 11 is maintained by Microsoft at servicing levels for specific periods of time to support Windows as a Service. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities which leaves them subject to exploitation.
New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 30 months depending on the release. Support for previously released versions has been extended for Enterprise editions.
A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates.

Solution

Update systems on the Semi-Annual Channel to 'Microsoft Windows 11 Version 22H2 (OS Build 22621.380)' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253263r1016364_rule
STIG-ID	WN11-00-000040
SWIFT-CSCV1	2.3
VULN-ID	V-253263

Assets

lognpacific3286

```
'26100'
```

WN11-00-000045 - The Windows 11 system must use an antivirus program.

Info

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.

Solution

Install Microsoft Defender Antivirus or a third-party antivirus solution.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253264r991589_rule
STIG-ID	WN11-00-000045
SWIFT-CSCV1	2.3
VULN-ID	V-253264

Assets

lognpacific3286

```
One of the following must pass to satisfy this requirement:

-------------------------
PASSED - Microsoft Defender Antivirus is installed:
 Remote value: 'Status DisplayName
 ------ -----------
Running Microsoft Defender Antivirus Network Inspection Service
Running Microsoft Defender Antivirus Service
PASS'
```

```
 Policy value: '^PASS$'


-------------------------
FAILED - Symantec Antivirus is installed:
 Remote value: 'FAIL - Symantec Antivirus not found'
 Policy value: '^PASS$'


-------------------------
FAILED - McAfee Antivirus is installed:
 Remote value: 'FAIL - McAfee Antivirus not found'
 Policy value: '^PASS$'
```

WN11-00-000050 - Local volumes must be formatted using NTFS.

Info

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

Solution

Format all local volumes to use NTFS.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	I
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20

ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253265r958472_rule
STIG-ID	WN11-00-000050
TBA-FIISB	31.1
VULN-ID	V-253265

Assets

lognpacific3286

```
'None'
```

WN11-00-000075 - Only accounts responsible for the backup operations must be members of the Backup Operators group.

Info

Backup Operators are able to read and write to any file in the system, regardless of the rights assigned to it. Backup and restore rights permit users to circumvent the file access restrictions present on NTFS disk drives for backup and restore purposes. Members of the Backup Operators group must have separate logon accounts for performing backup duties.

Solution

Create separate accounts for backup operations for users with this privilege.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253270r991589_rule
STIG-ID	WN11-00-000075
SWIFT-CSCV1	2.3
VULN-ID	V-253270

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Check if no accounts are members of the Backup Operators group.:
 Remote value: 'PASS: No accounts are part of the Backup Operators group.'
```

```
Policy value: 'PASS: No accounts are part of the Backup Operators group.'
```

WN11-00-000080 - Only authorized user accounts must be allowed to create or run virtual machines on Windows 11 systems.

Info

Allowing other operating systems to run on a secure system may allow users to circumvent security. For Hyper-V, preventing unauthorized users from being assigned to the Hyper-V Administrators group will prevent them from accessing or creating virtual machines on the system. The Hyper-V Hypervisor is used by virtualization-based Security features such as Credential Guard on Windows 11; however, it is not the full Hyper-V installation.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For Hyper-V, remove any unauthorized groups or user accounts from the 'Hyper-V Administrators' group.
For hosted hypervisors other than Hyper-V, restrict access to create or run virtual machines to authorized user accounts only.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	II
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33

ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253271r958702_rule
STIG-ID	WN11-00-000080
TBA-FIISB	31.1
VULN-ID	V-253271

Assets

lognpacific3286

```
'No entries found'
```

WN11-00-000085 - Standard local user accounts must not exist on a system in a domain.

Info

To minimize potential points of attack, local user accounts, other than built-in accounts and local administrator accounts, must not exist on a workstation in a domain. Users must log on to workstations in a domain with their domain accounts.

Solution

Limit local user accounts on domain-joined systems. Remove any unauthorized local accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253272r991589_rule
STIG-ID	WN11-00-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253272

Assets

lognpacific3286

PASSED

WN11-00-000095 - Permissions for system files and directories must conform to minimum requirements.

Info

Changing the system's file and directory permissions allows the possibility of unauthorized and anonymous modification to the operating system and installed applications.

Solution

Maintain the default file system permissions and configure the Security Option: 'Network access: Let everyone permissions apply to anonymous users' to 'Disabled' (WN11-SO-000160).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	II
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18

ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253274r1016661_rule
STIG-ID	WN11-00-000095
TBA-FIISB	31.1
VULN-ID	V-253274

Assets

lognpacific3286

PASSED

WN11-00-000100 - Internet Information System (IIS) or its subcomponents must not be installed on a workstation.

Info

IIS is not installed by default. Installation of Internet Information System (IIS) may allow unauthorized internet services to be hosted. Websites must only be hosted on servers that have been designed for that purpose and can be adequately secured.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Uninstall 'Internet Information Services' or 'Internet Information Services Hostable Web Core' from the system.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	I
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253275r958478_rule
STIG-ID	WN11-00-000100
SWIFT-CSCV1	2.3

VULN-ID V-253275

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - IIS-WebServer:
 Remote value: ''
 Policy value: '^Manual Review Required$'


-------------------------
PASSED - IIS-HostableWebCore:
 Remote value: ''
 Policy value: '^Manual Review Required$'
```

WN11-00-000105 - Simple Network Management Protocol (SNMP) must not be installed on the system.

Info

'SNMP' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Simple Network Management Protocol (SNMP)' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Simple Network Management Protocol (SNMP)'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253276r958480_rule
STIG-ID	WN11-00-000105
SWIFT-CSCV1	2.3
VULN-ID	V-253276

Assets

lognpacific3286

```
'%windir%\System32\snmp.exe_file_does_not_exist'
```

WN11-00-000110 - Simple TCP/IP Services must not be installed on the system.

Info

'Simple TCP/IP Services' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Simple TCPIP Services (i.e. echo, daytime etc.)' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Simple TCPIP Services (i.e. echo, daytime etc.)'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253277r958478_rule
STIG-ID	WN11-00-000110
SWIFT-CSCV1	2.3

VULN-ID	V-253277

Assets

lognpacific3286

```
'HKLM\System\CurrentControlSet\Services\Simptcp_registry_does_not_exist'
```

WN11-00-000115 - The Telnet Client must not be installed on the system.

Info

The 'Telnet Client' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'Telnet Client' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'Telnet Client'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253278r958480_rule
STIG-ID	WN11-00-000115
SWIFT-CSCV1	2.3
VULN-ID	V-253278

Assets

lognpacific3286

```
'%windir%\System32\telnet.exe_file_does_not_exist'
```

WN11-00-000120 - The TFTP Client must not be installed on the system.

Info

The 'TFTP Client' is not installed by default. Some protocols and services do not support required security features, such as encrypting passwords or traffic.

Solution

Uninstall 'TFTP Client' from the system.
Run 'Programs and Features'.
Select 'Turn Windows Features on or off'.
De-select 'TFTP Client'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06b.
800-53	CM-7b.
800-53R5	CM-7b.
CAT	II
CCI	CCI-000382
CN-L3	7.1.3.5(c)
CN-L3	7.1.3.7(d)
CN-L3	8.1.4.4(b)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS13b
NIAV2	SS14a
NIAV2	SS14c
PCI-DSSV3.2.1	2.2.2
PCI-DSSV4.0	2.2.4
QCSC-V1	3.2

RULE-ID	SV-253279r958480_rule
STIG-ID	WN11-00-000120
SWIFT-CSCV1	2.3
VULN-ID	V-253279

Assets

lognpacific3286

```
'%windir%\System32\TFTP.exe_file_does_not_exist'
```

WN11-00-000160 - The Server Message Block (SMB) v1 protocol must be disabled on the system.

Info

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.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older Network Attached Storage (NAS) devices may only support SMBv1.

Solution

Disable the SMBv1 protocol.
Run 'Windows PowerShell' with elevated privileges (run as administrator).
Enter the following:
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
Alternately:
Search for 'Features'.
Select 'Turn Windows features on or off'.
De-select 'SMB 1.0/CIFS File Sharing Support'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253286r958478_rule
STIG-ID	WN11-00-000160
SWIFT-CSCV1	2.3
VULN-ID	V-253286

Assets

lognpacific3286

```
'State : Disabled'
```

WN11-00-000165 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.

Info

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.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older network attached devices may only support SMBv1.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Configure SMBv1 Server' to 'Disabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories, respectively.
The system must be restarted for the change to take effect.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253287r958478_rule

STIG-ID	WN11-00-000165
SWIFT-CSCV1	2.3
VULN-ID	V-253287

Assets

lognpacific3286

PASSED

WN11-00-000170 - The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.

Info

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.
Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1. File shares and print services hosted on Windows Server 2003 are an example, however Windows Server 2003 is no longer a supported operating system. Some older network attached devices may only support SMBv1.

Solution

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'.
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.
The system must be restarted for the changes to take effect.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2

RULE-ID	SV-253288r958478_rule
STIG-ID	WN11-00-000170
SWIFT-CSCV1	2.3
VULN-ID	V-253288

Assets

lognpacific3286

PASSED

WN11-00-000210 - Bluetooth must be turned off unless approved by the organization.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.

Solution

Turn off Bluetooth radios not organizationally approved. Establish an organizational policy for the use of Bluetooth.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253291r958478_rule
STIG-ID	WN11-00-000210
SWIFT-CSCV1	2.3
VULN-ID	V-253291

Assets

lognpacific3286

```
'No entries found'
```

WN11-00-000220 - Bluetooth must be turned off when not in use.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.

Solution

Turn off Bluetooth radios when not in use. Establish an organizational policy for the use of Bluetooth to include training of personnel.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253292r958478_rule
STIG-ID	WN11-00-000220
SWIFT-CSCV1	2.3
VULN-ID	V-253292

Assets

lognpacific3286

```
'No entries found'
```

WN11-00-000395 - Windows 11 must not have portproxy enabled or in use.

Info

Having portproxy enabled or configured in Windows 10 could allow a man-in-the-middle attack.

Solution

Contact the Administrator to run 'netsh interface portproxy delete' with elevation. Remove any enabled portproxies that may be configured.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-257592r991589_rule
STIG-ID	WN11-00-000395
SWIFT-CSCV1	2.3
VULN-ID	V-257592

Assets

lognpacific3286

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - netsh:
 Remote value: 'Not found'
 Policy value: 'Not found'


-------------------------
PASSED - PortProxy:
 Remote value: 'HKLM\SYSTEM\CurrentControlSet\Services\PortProxy
\v4tov4\tcp_registry_does_not_exist'
 Policy value: 'HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp'
```

WN11-AC-000025 - The maximum password age must be configured to 60 days or less.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.07d.
800-53	IA-5(1)(d)
800-53R5	IA-5(1)(h)
CAT	II
CCI	CCI-000199
CCI	CCI-004066
CN-L3	7.1.2.7(e)
CN-L3	7.1.3.1(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ISO/IEC-27001	A.9.4.3
ITSG-33	IA-5(1)(d)
NESA	T5.2.3
NIAV2	AM20
NIAV2	AM21

QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253301r1051042_rule
STIG-ID	WN11-AC-000025
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-253301

Assets

lognpacific3286

42

WN11-AC-000045 - Reversible password encryption must be disabled.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(d)
CAT	I
CCI	CCI-000196
CCI	CCI-004062
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253305r1051046_rule
STIG-ID	WN11-AC-000045

SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253305

Assets

lognpacific3286

```
'disabled'
```

WN11-AU-000030 - The system must be configured to audit Account Management - Security Group Management successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03
800-53	AU-12(3)
800-53R5	AU-12(3)
CAT	II
CCI	CCI-001914
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ITSG-33	AU-12
PCI-DSSV3.2.1	10.1

QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253308r971541_rule
STIG-ID	WN11-AU-000030
SWIFT-CSCV1	6.4
VULN-ID	V-253308

Assets

lognpacific3286

```
'success'
```

WN11-AU-000040 - The system must be configured to audit Account Management - User Account Management successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.01
800-53	AC-2(4)
800-53R5	AC-2(4)
CAT	II
CCI	CCI-001403
CN-L3	7.1.3.2(d)
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	PR.AA-01
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18

ISO-27001-2022	A.8.2
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2(4)
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-253310r991551_rule
STIG-ID	WN11-AU-000040
TBA-FIISB	36.2.3
VULN-ID	V-253310

Assets

lognpacific3286

```
'success'
```

WN11-AU-000065 - The system must be configured to audit Logon/Logoff - Logoff successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.12
800-171R3	03.01.12
800-53	AC-17(1)
800-53R5	AC-17(1)
CAT	II
CCI	CCI-000067
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	PR.AC-3
CSF	PR.PT-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ITSG-33	AC-17(1)
NESA	T5.4.4
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2

RULE-ID	SV-253315r958406_rule
STIG-ID	WN11-AU-000065
SWIFT-CSCV1	2.6
VULN-ID	V-253315

Assets

lognpacific3286

```
'success'
```

WN11-AU-000070 - The system must be configured to audit Logon/Logoff - Logon failures.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253316r991581_rule
STIG-ID	WN11-AU-000070
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253316

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000075 - The system must be configured to audit Logon/Logoff - Logon successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253317r991581_rule
STIG-ID	WN11-AU-000075
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253317

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000080 - The system must be configured to audit Logon/Logoff - Special Logon successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253318r991578_rule
STIG-ID	WN11-AU-000080
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253318

Assets

lognpacific3286

```
'success'
```

WN11-AU-000100 - The system must be configured to audit Policy Change - Audit Policy Change successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253325r991572_rule
STIG-ID	WN11-AU-000100
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253325

Assets

lognpacific3286

```
'success'
```

WN11-AU-000105 - The system must be configured to audit Policy Change - Authentication Policy Change successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04

DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253326r991572_rule
STIG-ID	WN11-AU-000105
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253326

Assets

lognpacific3286

```
'success'
```

WN11-AU-000130 - The system must be configured to audit System - Other System Events successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253331r991579_rule
STIG-ID	WN11-AU-000130
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253331

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000135 - The system must be configured to audit System - Other System Events failures.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253332r991579_rule
STIG-ID	WN11-AU-000135
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253332

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000140 - The system must be configured to audit System - Security State Change successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG

GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253333r991575_rule
STIG-ID	WN11-AU-000140
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253333

Assets

lognpacific3286

```
'success'
```

WN11-AU-000155 - The system must be configured to audit System - System Integrity failures.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253335r991573_rule
STIG-ID	WN11-AU-000155
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253335

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000160 - The system must be configured to audit System - System Integrity successes.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171R3	03.03.03a.
800-53	AU-12c.
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253336r991573_rule
STIG-ID	WN11-AU-000160
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253336

Assets

lognpacific3286

```
'success, failure'
```

WN11-AU-000515 - Windows 11 permissions for the Application event log must prevent access by non-privileged accounts.

Info

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

Solution

Ensure the permissions on the Application event log (Application.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253340r958434_rule
STIG-ID	WN11-AU-000515
VULN-ID	V-253340

Assets

lognpacific3286

```
'C:\Windows\System32\winevt\Logs\Application.evtx NT SERVICE\EventLog:(I)(F)
                                                  NT AUTHORITY\SYSTEM:(I)(F)
                                                  BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-AU-000520 - Windows 11 permissions for the Security event log must prevent access by non-privileged accounts.

Info

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

Solution

Ensure the permissions on the Security event log (Security.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253341r958434_rule
STIG-ID	WN11-AU-000520
VULN-ID	V-253341

Assets

lognpacific3286

```
'C:\Windows\System32\winevt\Logs\Security.evtx NT SERVICE\EventLog:(I)(F)
                                               NT AUTHORITY\SYSTEM:(I)(F)
                                               BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-AU-000525 - Windows 11 permissions for the System event log must prevent access by non-privileged accounts.

Info

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

Solution

Ensure the permissions on the System event log (System.evtx) are configured to prevent standard user accounts or groups from having access. The default permissions listed below satisfy this requirement.
Eventlog - Full Control SYSTEM - Full Control Administrators - Full Control
The default location is the '%SystemRoot%\SYSTEM32\WINEVT\LOGS' directory.
If the location of the logs has been changed, when adding Eventlog to the permissions, it must be entered as 'NT Service\Eventlog'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9a.
CAT	II
CCI	CCI-000162
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	PR.PT-1
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
NESA	M5.2.3

NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253342r958434_rule
STIG-ID	WN11-AU-000525
VULN-ID	V-253342

Assets

lognpacific3286

```
'C:\Windows\System32\winevt\Logs\System.evtx NT SERVICE\EventLog:(I)(F)
                                             NT AUTHORITY\SYSTEM:(I)(F)
                                             BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN11-CC-000037 - Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.

Info

A compromised local administrator account can provide means for an attacker to move laterally between domain systems.
With User Account Control enabled, filtering the privileged token for built-in administrator accounts will prevent the elevated privileges of these accounts from being used over the network.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Apply UAC restrictions to local accounts on network logons' to 'Enabled'.
This policy setting requires the installation of the SecGuide custom templates included with the STIG package. 'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows \PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253357r958518_rule
STIG-ID	WN11-CC-000037
VULN-ID	V-253357

Assets

lognpacific3286

PASSED

WN11-CC-000055 - Simultaneous connections to the internet or a Windows domain must be limited.

Info

Multiple network connections can provide additional attack vectors to a system and must be limited. The 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' setting prevents systems from automatically establishing multiple connections. When both wired and wireless connections are available, for example, the less preferred connection (typically wireless) will be disconnected.

Solution

The default behavior for 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is 'Enabled'.
If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Network >> Windows Connection Manager >> 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' to 'Enabled'. Under 'Options', set 'Minimize Policy Options' to '3 = Prevent Wi-Fi When on Ethernet'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)

ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253364r958358_rule
STIG-ID	WN11-CC-000055
VULN-ID	V-253364

Assets

lognpacific3286

NULL

WN11-CC-000063 - Windows 11 systems must use either Group Policy or an approved Mobile Device Management (MDM) product to enforce STIG compliance.

Info

Without Windows 11 systems being managed, devices could be rogue and become targets of an attacker.

Solution

Configure the Windows 11 system to use either Group Policy or an approved MDM product to enforce STIG compliance.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-268318r1081062_rule
STIG-ID	WN11-CC-000063
SWIFT-CSCV1	2.3
VULN-ID	V-268318

Assets

lognpacific3286

PASSED

WN11-CC-000075 - Credential Guard must be running on Windows 11 domain-joined systems.

Info

Credential Guard uses virtualization-based security to protect information that could be used in credential theft attacks if compromised. This authentication information, which was stored in the Local Security Authority (LSA) in previous versions of Windows, is isolated from the rest of operating system and can only be accessed by privileged system software.

Solution

Virtualization-based security, including Credential Guard, currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
For VDIs with persistent desktops, this may be downgraded to a CAT II only where administrators have specific tokens for the VDI. Administrator accounts on virtual desktops must only be used on systems in the VDI; they may not have administrative privileges on any other systems such as servers and physical workstations.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Enabled with UEFI lock' selected for 'Credential Guard Configuration:'.
A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link:
https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253370r991589_rule
STIG-ID	WN11-CC-000075

SWIFT-CSCV1	2.3
VULN-ID	V-253370

Assets

lognpacific3286

PASSED

WN11-CC-000080 - Virtualization-based protection of code integrity must be enabled.

Info

Virtualization-based protection of code integrity enforces kernel mode memory protections as well as protecting Code Integrity validation paths. This isolates the processes from the rest of the operating system and can only be accessed by privileged system software.

Solution

Virtualization-based security currently cannot be implemented in virtual desktop implementations (VDI) due to specific supporting requirements including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.
For VDIs where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Device Guard >> 'Turn On virtualization-based Security' to 'Enabled' with 'Enabled with UEFI lock' or 'Enabled without lock' selected for 'virtualization-based Protection of Code Integrity:'.
'Enabled with UEFI lock' is preferred as more secure, however it cannot be turned off remotely through a group policy change if there is an issue.
'Enabled without lock' will allow this to be turned off remotely while testing for issues.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253371r991589_rule
STIG-ID	WN11-CC-000080
SWIFT-CSCV1	2.3
VULN-ID	V-253371

Assets

lognpacific3286

PASSED

WN11-CC-000115 - Systems must at least attempt device authentication using certificates.

Info

Using certificates to authenticate devices to the domain provides increased security over passwords. By default systems will attempt to authenticate using certificates and fall back to passwords if the domain controller does not support certificates for devices. This may also be configured to always use certificates for device authentication.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
The default behavior for 'Support device authentication using certificate' is 'Automatic'.
To correct this, configured the policy value for Computer Configuration >> Administrative Templates >> System >> Kerberos >> 'Support device authentication using certificate' to 'Not Configured or 'Enabled' with either option selected in 'Device authentication behavior using certificate:'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253377r991589_rule
STIG-ID	WN11-CC-000115
SWIFT-CSCV1	2.3
VULN-ID	V-253377

Assets

lognpacific3286

PASSED

WN11-CC-000130 - Local users on domain-joined computers must not be enumerated.

Info

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

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Logon >> 'Enumerate local users on domain-joined computers' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253379r958478_rule
STIG-ID	WN11-CC-000130
SWIFT-CSCV1	2.3
VULN-ID	V-253379

Assets

lognpacific3286

PASSED

WN11-CC-000215 - Explorer Data Execution Prevention must be enabled.

Info

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

Solution

The default behavior is for data execution prevention to be turned on for file explorer.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off Data Execution Prevention for Explorer' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	II
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-253396r958928_rule
STIG-ID	WN11-CC-000215
VULN-ID	V-253396

Assets

lognpacific3286

NULL

WN11-CC-000220 - File Explorer heap termination on corruption must be disabled.

Info

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

Solution

The default behavior is for File Explorer heap termination on corruption to be enabled.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off heap termination on corruption' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-5
800-53R5	SC-5a.
CAT	III
CCI	CCI-002385
CSF	DE.CM-1
CSF	PR.DS-4
CSF2.0	DE.CM-01
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-5
ITSG-33	SC-5a.
NESA	T3.3.1
NIAV2	GS8e
NIAV2	GS10c
QCSC-V1	8.2.1
RULE-ID	SV-253397r958902_rule
STIG-ID	WN11-CC-000220
VULN-ID	V-253397

Assets

lognpacific3286

```
NULL
```

WN11-CC-000225 - File Explorer shell protocol must run in protected mode.

Info

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

Solution

The default behavior is for shell protected mode to be turned on for file explorer.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Turn off shell protocol protected mode' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253398r991589_rule
STIG-ID	WN11-CC-000225
SWIFT-CSCV1	2.3
VULN-ID	V-253398

Assets

lognpacific3286

```
NULL
```

WN11-CC-000300 - Basic authentication for RSS feeds over HTTP must not be used.

Info

Basic authentication uses plain text passwords that could be used to compromise a system.

Solution

The default behavior is for the Windows RSS platform to not use Basic authentication over HTTP connections. To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> 'Turn on Basic feed authentication over HTTP' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.6
800-171	3.4.7
800-171R3	03.04.06a.
800-53	CM-7a.
800-53R5	CM-7a.
CAT	II
CCI	CCI-000381
CN-L3	7.1.3.5(c)
CN-L3	8.1.4.4(a)
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7a.
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.1
PCI-DSSV4.0	2.2.3
QCSC-V1	3.2
RULE-ID	SV-253408r958478_rule
STIG-ID	WN11-CC-000300
SWIFT-CSCV1	2.3
VULN-ID	V-253408

Assets

lognpacific3286

```
NULL
```

WN11-CC-000320 - Users must be notified if a web-based program attempts to install software.

Info

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

Solution

The default behavior is for Internet Explorer to warn users and select whether to allow or refuse installation when a web-based program attempts to install software on the system.
To correct this, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> 'Prevent Internet Explorer security prompt for Windows Installer scripts' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253412r991589_rule
STIG-ID	WN11-CC-000320
SWIFT-CSCV1	2.3
VULN-ID	V-253412

Assets

lognpacific3286

```
NULL
```

WN11-RG-000005 - Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.

Info

The registry is integral to the function, security, and stability of the Windows system. Changing the system's registry permissions allows the possibility of unauthorized and anonymous modification to the operating system.

Solution

Maintain the default permissions for the HKEY_LOCAL_MACHINE registry hive.
The default permissions of the higher level keys are noted below.
HKEY_LOCAL_MACHINE\SECURITY Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to SYSTEM - Full Control - This key and subkeys Administrators - Special - This key and subkeys
HKEY_LOCAL_MACHINE\SOFTWARE Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to Users - Read - This key and subkeys Administrators - Full Control - This key and subkeys SYSTEM - Full Control - This key and subkeys CREATOR OWNER - Full Control - This key and subkeys ALL APPLICATION PACKAGES - Read - This key and subkeys
HKEY_LOCAL_MACHINE\SYSTEM Type - 'Allow' for all Inherited from - 'None' for all Principal - Access - Applies to Users - Read - This key and subkeys Administrators - Full Control - This key and subkeys SYSTEM - Full Control - This key and subkeys CREATOR OWNER - Full Control - This key and subkeys ALL APPLICATION PACKAGES - Read - This key and subkeys
Microsoft has also given read permission to the SOFTWARE and SYSTEM registry keys in later versions of Windows 11 to the following SID.
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2

ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253431r958726_rule
STIG-ID	WN11-RG-000005
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253431

Assets

lognpacific3286

```
 All of the following must pass to satisfy this requirement:

-------------------------
PASSED - HKEY_LOCAL_MACHINE\SECURITY:
 Remote value:

  administrators:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'read control' | 'write dac'

  system:
  + Apply To: 'this key and subkeys'
```

```
   |- Inheritance: 'not inherited'
   |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write dac' | 'write owner'


 Policy value:

 administrators:
  + Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'read control' | 'write dac'

 system:
  + Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write dac' | 'write owner'




-------------------------
PASSED - HKEY_LOCAL_MACHINE\SOFTWARE:
 Remote value:


 1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'enumerate subkeys' | 'notify' | 'query value' | 'read control'

  administrators:
  + Apply To: 'this key and subkeys'
   |- Inheritance: 'not inherited'
   |- Allow: 'create link' | 'create subkey' | 'delete' | 'enumerate subkeys' | 'full control' |
 'notify' | 'query value' | 'read control' | 'set value' | 'write [...]
```

WN11-SO-000015 - Local accounts with blank passwords must be restricted to prevent access from the network.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253434r991589_rule
STIG-ID	WN11-SO-000015
SWIFT-CSCV1	2.3
VULN-ID	V-253434

Assets

lognpacific3286

1

WN11-SO-000020 - The built-in administrator account must be renamed.

Info

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.

Solution

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'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253435r991589_rule
STIG-ID	WN11-SO-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253435

Assets

lognpacific3286

```
'SantiagoX86'
```

WN11-SO-000035 - Outgoing secure channel traffic must be encrypted or signed.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253438r958908_rule
STIG-ID	WN11-SO-000035

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253438

Assets

lognpacific3286

1

WN11-SO-000040 - Outgoing secure channel traffic must be encrypted.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253439r958908_rule
STIG-ID	WN11-SO-000040

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253439

Assets

lognpacific3286

1

WN11-SO-000045 - Outgoing secure channel traffic must be signed.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53	SC-8(1)
800-53R5	SC-8
800-53R5	SC-8(1)
CAT	II
CCI	CCI-002418
CCI	CCI-002421
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)

HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.10.1.1
ISO/IEC-27001	A.13.2.3
ITSG-33	SC-8
ITSG-33	SC-8a.
ITSG-33	SC-8(1)
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS5d
NIAV2	NS6b
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253440r958908_rule
STIG-ID	WN11-SO-000045

SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-253440

Assets

lognpacific3286

1

WN11-SO-000050 - The computer account password must not be prevented from being reset.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253441r991589_rule
STIG-ID	WN11-SO-000050
SWIFT-CSCV1	2.3
VULN-ID	V-253441

Assets

lognpacific3286

0

WN11-SO-000055 - The maximum age for machine account passwords must be configured to 30 days or less.

Info

Computer account passwords are changed automatically on a regular basis. This setting controls the maximum password age that a machine account may have. This setting must be set to no more than 30 days, ensuring the machine changes its password monthly.

Solution

This is the default configuration for this setting (30 days).
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Maximum machine account password age' to '30' or less (excluding 0 which is unacceptable).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253442r991589_rule
STIG-ID	WN11-SO-000055
SWIFT-CSCV1	2.3
VULN-ID	V-253442

Assets

lognpacific3286

```
30
```

WN11-SO-000060 - The system must be configured to require a strong session key.

Info

A computer connecting to a domain controller will establish a secure channel. Requiring strong session keys enforces 128-bit encryption between systems.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Domain member: Require strong (Windows 2000 or Later) session key' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8
800-53R5	SC-8
CAT	II
CCI	CCI-002418
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
CN-L3	8.1.4.7(a)
CN-L3	8.1.4.8(a)
CN-L3	8.2.4.5(c)
CN-L3	8.2.4.5(d)
CN-L3	8.5.2.2
CSF	PR.DS-2
CSF	PR.DS-5
CSF2.0	PR.DS-02
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.14

ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.20
ITSG-33	SC-8
ITSG-33	SC-8a.
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
PCI-DSSV3.2.1	2.3
PCI-DSSV3.2.1	4.1
PCI-DSSV4.0	2.2.7
PCI-DSSV4.0	4.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253443r958908_rule
STIG-ID	WN11-SO-000060
VULN-ID	V-253443

Assets

lognpacific3286

1

WN11-SO-000085 - Caching of logon credentials must be limited.

Info

The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons, such as the user's machine being disconnected from the network or domain controllers being unavailable. Even though the credential cache is well-protected, if a system is attacked, an unauthorized individual may isolate the password to a domain user account using a password-cracking program and gain access to the domain.

Solution

This is the default configuration for this setting (10 logons to cache).
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '10' logons or less.
This setting only applies to domain-joined systems, however, it is configured by default on all systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253447r991589_rule
STIG-ID	WN11-SO-000085
SWIFT-CSCV1	2.3
VULN-ID	V-253447

Assets

lognpacific3286

PASSED

WN11-SO-000110 - Unencrypted passwords must not be sent to third-party SMB Servers.

Info

Some non-Microsoft SMB servers only support unencrypted (plain text) password authentication. Sending plain text passwords across the network, when authenticating to an SMB server, reduces the overall security of the environment. Check with the vendor of the SMB server to see if there is a way to support encrypted password authentication.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(c)
CAT	II
CCI	CCI-000197
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253450r987796_rule
STIG-ID	WN11-SO-000110

SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253450

Assets

lognpacific3286

```
0
```

WN11-SO-000140 - Anonymous SID/Name translation must not be allowed.

Info

Allowing anonymous SID/Name translation can provide sensitive information for accessing a system. Only authorized users must be able to perform such translations.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Allow anonymous SID/Name translation' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253452r991589_rule
STIG-ID	WN11-SO-000140
SWIFT-CSCV1	2.3
VULN-ID	V-253452

Assets

lognpacific3286

```
'disabled'
```

WN11-SO-000145 - Anonymous enumeration of SAM accounts must not be allowed.

Info

Anonymous enumeration of SAM accounts allows anonymous log on users (null session connections) to list all accounts names, thus providing a list of potential points to attack the system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253453r991589_rule
STIG-ID	WN11-SO-000145
SWIFT-CSCV1	2.3
VULN-ID	V-253453

Assets

lognpacific3286

1

WN11-SO-000160 - The system must be configured to prevent anonymous users from having the same rights as the Everyone group.

Info

Access by anonymous users must be restricted. If this setting is enabled, then anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users must not have these permissions or rights.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253455r991589_rule
STIG-ID	WN11-SO-000160
SWIFT-CSCV1	2.3
VULN-ID	V-253455

Assets

lognpacific3286

0

WN11-SO-000165 - Anonymous access to Named Pipes and Shares must be restricted.

Info

Allowing anonymous access to named pipes or shares provides the potential for unauthorized system access. This setting restricts access to those defined in 'Network access: Named Pipes that can be accessed anonymously' and 'Network access: Shares that can be accessed anonymously', both of which must be blank under other requirements.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	I
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253456r958524_rule
STIG-ID	WN11-SO-000165
VULN-ID	V-253456

Assets

lognpacific3286

1

WN11-SO-000195 - The system must be configured to prevent the storage of the LAN Manager hash of passwords.

Info

The LAN Manager hash uses a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords. This setting controls whether or not a LAN Manager hash of the password is stored in the SAM the next time the password is changed.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.10
800-171R3	03.05.07c.
800-53	IA-5(1)(c)
800-53R5	IA-5(1)(d)
CAT	I
CCI	CCI-000196
CCI	CCI-004062
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.17
ITSG-33	IA-5(1)(c)
NESA	T5.2.3
NIAV2	CY6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253461r1051056_rule

STIG-ID	WN11-SO-000195
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-253461

Assets

lognpacific3286

1

WN11-SO-000210 - The system must be configured to the required LDAP client signing level.

Info

This setting controls the signing requirements for LDAP clients. This setting must be set to Negotiate signing or Require signing, depending on the environment and type of LDAP server in use.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: LDAP client signing requirements' to 'Negotiate signing' at a minimum.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253463r991589_rule
STIG-ID	WN11-SO-000210
SWIFT-CSCV1	2.3
VULN-ID	V-253463

Assets

lognpacific3286

1

WN11-SO-000240 - The default permissions of global system objects must be increased.

Info

Windows systems maintain a global list of shared system resources such as DOS device names, mutexes, and semaphores. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	III
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253467r991589_rule
STIG-ID	WN11-SO-000240
SWIFT-CSCV1	2.3
VULN-ID	V-253467

Assets

lognpacific3286

1

WN11-SO-000251 - Windows 11 must use multifactor authentication for local and network access to privileged and nonprivileged accounts.

Info

Without the use of multifactor authentication, the ease of access to privileged and nonprivileged functions is greatly increased.
All domain accounts must be enabled for multifactor authentication with the exception of local emergency accounts.
Multifactor authentication requires using two or more factors to achieve authentication.
Factors include:
1) Something a user knows (e.g., password/PIN);
2) Something a user has (e.g., cryptographic identification device, token); and
3) Something a user is (e.g., biometric).
A privileged account is defined as an information system account with authorizations of a privileged user.
Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).
Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
The DoD CAC with DoD-approved PKI is an example of multifactor authentication.
Satisfies: SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Solution

For nondomain joined systems, configuring Windows Hello for sign-on options would be suggested based on the organization's needs and capabilities.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.5.3
800-171R3	03.05.03
800-53	IA-2(1)
800-53R5	IA-2(1)
CAT	II
CCI	CCI-000765
CN-L3	7.1.2.7(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ITSG-33	IA-2(1)
NESA	T5.4.2

NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253470r1106510_rule
STIG-ID	WN11-SO-000251
SWIFT-CSCV1	1.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-253470

Assets

lognpacific3286

PASSED

WN11-SO-000260 - User Account Control must be configured to detect application installations and prompt for elevation.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting requires Windows to respond to application installation requests by prompting for credentials.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253472r958518_rule
STIG-ID	WN11-SO-000260
VULN-ID	V-253472

Assets

lognpacific3286

1

WN11-SO-000265 - User Account Control must only elevate UIAccess applications that are installed in secure locations.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures Windows to only allow applications installed in a secure location on the file system, such as the Program Files or the Windows\System32 folders, to run with elevated privileges.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253473r958518_rule
STIG-ID	WN11-SO-000265
VULN-ID	V-253473

Assets

lognpacific3286

1

WN11-SO-000270 - User Account Control must run all administrators in Admin Approval Mode, enabling UAC.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting enables UAC.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171R3	03.05.01b.
800-53	IA-11
800-53R5	IA-11
CAT	II
CCI	CCI-002038
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-253474r1051059_rule
STIG-ID	WN11-SO-000270
VULN-ID	V-253474

Assets

lognpacific3286

1

WN11-SO-000275 - User Account Control must virtualize file and registry write failures to per-user locations.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting configures non-UAC compliant applications to run in virtualized file and registry entries in per-user locations, allowing them to run.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-3
ITSG-33	SC-3a.
NESA	T3.4.1
NESA	T4.3.1
NESA	T4.3.2
RULE-ID	SV-253475r958518_rule
STIG-ID	WN11-SO-000275
VULN-ID	V-253475

Assets

lognpacific3286

1

WN11-UC-000020 - Zone information must be preserved when saving attachments.

Info

Preserving zone of origin (internet, intranet, local, restricted) information on file attachments allows Windows to determine risk.

Solution

The default behavior is for Windows to mark file attachments with their zone information.
To correct this, configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Attachment Manager >> 'Do not preserve zone information in file attachments' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253478r991589_rule
STIG-ID	WN11-UC-000020
SWIFT-CSCV1	2.3
VULN-ID	V-253478

Assets

lognpacific3286

```
Compliant items:
  HKU\S-1-5-21-108538807-2850267539-2289239689-500\Software\Microsoft\Windows\Currentversion
\Policies\Attachments -
```

WN11-UR-000005 - The 'Access Credential Manager as a trusted caller' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Access Credential Manager as a trusted caller' user right may be able to retrieve the credentials of other accounts from Credential Manager.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Access Credential Manager as a trusted caller' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253479r958726_rule
STIG-ID	WN11-UR-000005
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253479

Assets

lognpacific3286

```
NULL
```

WN11-UR-000015 - The 'Act as part of the operating system' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Act as part of the operating system' user right can assume the identity of any user and gain access to resources that user is authorized to access. Any accounts with this right can take complete control of a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Act as part of the operating system' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253481r958726_rule
STIG-ID	WN11-UR-000015
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253481

Assets

lognpacific3286

```
NULL
```

WN11-UR-000035 - The 'Change the system time' user right must only be assigned to Administrators and Local Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Change the system time' user right can change the system time, which can impact authentication, as well as affect time stamps on event log entries.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Change the system time' to only include the following groups or accounts:
Administrators LOCAL SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253484r958726_rule
STIG-ID	WN11-UR-000035
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253484

Assets

lognpacific3286

```
'administrators' && 'local service'
```

WN11-UR-000040 - The 'Create a pagefile' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create a pagefile' user right can change the size of a pagefile, which could affect system performance.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create a pagefile' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253485r958726_rule
STIG-ID	WN11-UR-000040
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253485

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000045 - The 'Create a token object' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Create a token object' user right allows a process to create an access token. This could be used to provide elevated rights and compromise a system.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create a token object' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253486r958726_rule
STIG-ID	WN11-UR-000045
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253486

Assets

lognpacific3286

```
NULL
```

WN11-UR-000050 - The 'Create global objects' user right must only be assigned to Administrators, Service, Local Service, and Network Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Create global objects' user right can create objects that are available to all sessions, which could affect processes in other users' sessions.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create global objects' to only include the following groups or accounts:
Administrators LOCAL SERVICE NETWORK SERVICE SERVICE

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253487r958726_rule
STIG-ID	WN11-UR-000050
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253487

Assets

lognpacific3286

```
'service' && 'administrators' && 'network service' && 'local service'
```

WN11-UR-000055 - The 'Create permanent shared objects' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create permanent shared objects' user right could expose sensitive data by creating shared objects.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create permanent shared objects' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253488r958726_rule
STIG-ID	WN11-UR-000055
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253488

Assets

lognpacific3286

```
NULL
```

WN11-UR-000060 - The 'Create symbolic links' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Create symbolic links' user right can create pointers to other objects, which could potentially expose the system to attack.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Create symbolic links' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253489r958726_rule
STIG-ID	WN11-UR-000060
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253489

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000065 - The 'Debug programs' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Debug Programs' user right can attach a debugger to any process or to the kernel, providing complete access to sensitive and critical operating system components. This right is given to Administrators in the default configuration.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Debug programs' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	I
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2

NESA	T5.4.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253490r958726_rule
STIG-ID	WN11-UR-000065
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253490

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000075 - The 'Deny log on as a batch job' user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on as a batch job' right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a batch job' to include the following:
Domain Systems Only:
Enterprise Admin Group Domain Admin Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253492r958472_rule
STIG-ID	WN11-UR-000075
TBA-FIISB	31.1
VULN-ID	V-253492

Assets

lognpacific3286

PASSED

WN11-UR-000080 - The 'Deny log on as a service' user right on Windows 11 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Deny log on as a service' right defines accounts that are denied log on as a service.
In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower trust systems helps mitigate the risk of privilege escalation from credential theft attacks which could lead to the compromise of an entire domain.
Incorrect configurations could prevent services from starting and result in a DoS.

Solution

This requirement is applicable to domain-joined systems, for standalone systems this is NA.
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a service' to include the following:
Domain Systems Only:
Enterprise Admins Group Domain Admins Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	II
CCI	CCI-000213
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253493r958472_rule
STIG-ID	WN11-UR-000080
TBA-FIISB	31.1
VULN-ID	V-253493

Assets

lognpacific3286

PASSED

WN11-UR-000095 - The 'Enable computer and user accounts to be trusted for delegation' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Enable computer and user accounts to be trusted for delegation' user right allows the 'Trusted for Delegation' setting to be changed. This could potentially allow unauthorized users to impersonate other users.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Enable computer and user accounts to be trusted for delegation' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253496r958726_rule
STIG-ID	WN11-UR-000095
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253496

Assets

lognpacific3286

```
NULL
```

WN11-UR-000100 - The 'Force shutdown from a remote system' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Force shutdown from a remote system' user right can remotely shut down a system which could result in a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Force shutdown from a remote system' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253497r958726_rule
STIG-ID	WN11-UR-000100
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253497

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000120 - The 'Load and unload device drivers' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Load and unload device drivers' user right allows device drivers to dynamically be loaded on a system by a user.
This could potentially be used to install malicious code by an attacker.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Load and unload device drivers' to only include the following groups or accounts:
Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253499r958726_rule
STIG-ID	WN11-UR-000120
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253499

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000125 - The 'Lock pages in memory' user right must not be assigned to any groups or accounts.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
The 'Lock pages in memory' user right allows physical memory to be assigned to processes, which could cause performance issues or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Lock pages in memory' to be defined but containing no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253500r958726_rule
STIG-ID	WN11-UR-000125
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253500

Assets

lognpacific3286

```
NULL
```

WN11-UR-000130 - The 'Manage auditing and security log' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Manage auditing and security log' user right can manage the security log and change auditing configurations. This could be used to clear evidence of tampering.
Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000063-GPOS-00032

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Manage auditing and security log' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.8
800-171R3	03.03.03
800-171R3	03.03.08
800-53	AU-9
800-53	AU-12b.
800-53R5	AU-9a.
800-53R5	AU-12b.
CAT	II
CCI	CCI-000162
CCI	CCI-000171
CN-L3	7.1.2.3(d)
CN-L3	7.1.3.3(f)
CN-L3	8.1.3.5(c)
CN-L3	8.1.4.3(c)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03

CSF2.0	DE.CM-09
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.2
ITSG-33	AU-9
ITSG-33	AU-12b.
NESA	M5.2.3
NESA	M5.5.2
NESA	T3.6.4
NESA	T8.2.9
NIAV2	SM5
NIAV2	SM6
PCI-DSSV3.2.1	10.1
PCI-DSSV3.2.1	10.5
PCI-DSSV3.2.1	10.5.2
PCI-DSSV4.0	10.3.2
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-253501r958434_rule
STIG-ID	WN11-UR-000130
SWIFT-CSCV1	6.4
VULN-ID	V-253501

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000140 - The 'Modify firmware environment values' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Modify firmware environment values' user right can change hardware configuration environment variables. This could result in hardware failures or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Modify firmware environment values' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253502r958726_rule
STIG-ID	WN11-UR-000140
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253502

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000145 - The 'Perform volume maintenance tasks' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.
Accounts with the 'Perform volume maintenance tasks' user right can manage volume and disk configurations. They could potentially delete volumes, resulting in data loss or a DoS.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Perform volume maintenance tasks' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253503r958726_rule
STIG-ID	WN11-UR-000145
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253503

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000150 - The 'Profile single process' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Profile single process' user right can monitor non-system processes performance. An attacker could potentially use this to identify processes to attack.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Profile single process' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253504r958726_rule
STIG-ID	WN11-UR-000150
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253504

Assets

lognpacific3286

```
'administrators'
```

WN11-UR-000165 - The 'Take ownership of files or other objects' user right must only be assigned to the Administrators group.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Take ownership of files or other objects' user right can take ownership of objects and make changes.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Take ownership of files or other objects' to only include the following groups or accounts: Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.7
800-171R3	03.01.07a.
800-53	AC-6(10)
800-53R5	AC-6(10)
CAT	II
CCI	CCI-002235
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
CN-L3	8.1.4.2(d)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
CSF2.0	PR.AA-05
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.18
ITSG-33	AC-6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.4.1

NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253506r958726_rule
STIG-ID	WN11-UR-000165
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-253506

Assets

lognpacific3286

```
'administrators'
```

Audits INFO,WARNING,ERROR

WN11-00-000025 - Windows 11 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: Continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Info

An approved tool for continuous network scanning must be installed and configured to run.
Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.
To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools, as specified in the requirement.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Install DOD-approved ESS software and ensure it is operating continuously.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253258r1000099_rule
STIG-ID	WN11-00-000025
SWIFT-CSCV1	2.3
VULN-ID	V-253258

Assets

lognpacific3286

WN11-00-000030 - Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.

Info

If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Enable full disk encryption on all information systems (including SIPRNet) using BitLocker.
BitLocker, included in Windows, can be enabled in the Control Panel under 'BitLocker Drive Encryption' as well as other management tools.
Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28(1)
800-53R5	SC-28(1)
CAT	I
CCI	CCI-002475
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.33
ITSG-33	SC-28(1)
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1

QCSC-V1	5.2.2
QCSC-V1	6.2
RULE-ID	SV-253259r958870_rule
STIG-ID	WN11-00-000030
TBA-FIISB	28.1
VULN-ID	V-253259

Assets

lognpacific3286

```
'VolumeType       : OperatingSystem
MountPoint       : C:
ProtectionStatus : Off

VolumeType       : Data
MountPoint       : D:
ProtectionStatus : Off



Some disks not encrypted.'
```

WN11-00-000035 - The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Info

Utilizing an allowlist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.
The organization must identify authorized software programs and only permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allowlisting.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure an application allowlisting program to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.
Configuration of allowlisting applications will vary by the program. AppLocker is an allowlisting application built into Windows 11 Enterprise.
If AppLocker is used, it is configured through group policy in Computer Configuration >> Windows Settings >> Security Settings >> Application Control Policies >> AppLocker.
Implementation guidance for AppLocker is available in the NSA paper 'Application allowlisting using Microsoft AppLocker' at the following link:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.8
800-171R3	03.04.08b.
800-53	CM-7(5)(b)
800-53R5	CM-7(5)(b)
CAT	II
CCI	CCI-001774
CSF	PR.IP-1
CSF	PR.PT-3
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.19
ISO/IEC-27001	A.12.5.1
ISO/IEC-27001	A.12.6.2
ITSG-33	CM-7
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2

QCSC-V1	3.2
RULE-ID	SV-253262r958808_rule
STIG-ID	WN11-00-000035
SWIFT-CSCV1	2.3
TBA-FIISB	44.2.2
TBA-FIISB	49.2.3
VULN-ID	V-253262

Assets

lognpacific3286

```
'<AppLockerPolicy Version="1" />'
```

WN11-00-000055 - Alternate operating systems must not be permitted on the same system.

Info

Allowing other operating systems to run on a secure system may allow security to be circumvented.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Ensure Windows 11 is the only operating system on a device. Remove alternate operating systems.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253266r991589_rule
STIG-ID	WN11-00-000055
SWIFT-CSCV1	2.3
VULN-ID	V-253266

Assets

lognpacific3286

WN11-00-000060 - Non-system-created file shares on a system must limit access to groups that require it.

Info

Shares which provide network access, must not exist on a workstation except for system-created administrative shares, and could potentially expose sensitive information. If a share is necessary, share permissions, as well as NTFS permissions, must be reconfigured to give the minimum access to those accounts that require it.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

If a non-system-created share is required on a system, configure the share and NTFS permissions to limit access to the specific groups or accounts that require it.
Remove any unnecessary non-system-created shares.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.4
800-171R3	03.13.04
800-53	SC-4
800-53R5	SC-4
CAT	II
CCI	CCI-001090
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-253267r958524_rule
STIG-ID	WN11-00-000060
VULN-ID	V-253267

Assets

lognpacific3286

WN11-00-000065 - Unused accounts must be disabled or removed from the system after 35 days of inactivity.

Info

Outdated or unused accounts provide penetration points that may go undetected. Inactive accounts must be deleted if no longer necessary or, if still required, disable until needed.
Satisfies: SRG-OS-000468-GPOS-00212, SRG-OS-000118-GPOS-00060
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Review local accounts and verify their necessity. Disable or delete any active accounts that have not been used in the last 35 days.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.5.5
800-171	3.5.6
800-171R3	03.03.03a.
800-171R3	03.05.05
800-53	AU-12c.
800-53	IA-4e.
800-53R5	AC-2(3)(a)
800-53R5	AU-12c.
CAT	III
CCI	CCI-000172
CCI	CCI-000795
CCI	CCI-003627
CN-L3	7.1.2.7(b)
CN-L3	7.1.3.3(a)
CN-L3	7.1.3.3(b)
CN-L3	7.1.3.3(c)
CN-L3	8.1.3.5(a)
CN-L3	8.1.3.5(b)
CN-L3	8.1.4.3(a)
CSF	DE.CM-1
CSF	DE.CM-3

CSF	DE.CM-7
CSF	PR.AC-1
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-01
CSF2.0	PR.PS-04
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(b)
HIPAA	164.312(d)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	IA-4e.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NIAV2	SM8
PCI-DSSV3.2.1	8.1.4
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	8.2.6
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

RULE-ID	SV-253268r1051039_rule
STIG-ID	WN11-00-000065
SWIFT-CSCV1	5
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-253268

Assets

lognpacific3286

WN11-00-000070 - Only accounts responsible for the administration of a system must have Administrator rights on the system.

Info

An account that does not have Administrator duties must not have Administrator rights. Such rights would allow the account to bypass or modify required security restrictions on that machine and make it vulnerable to attack.
System administrators must log on to systems only using accounts with the minimum level of authority necessary.
For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group (see V-36434 in the Active Directory Domain STIG). Restricting highly privileged accounts from the local Administrators group helps mitigate the risk of privilege escalation resulting from credential theft attacks.
Standard user accounts must not be members of the local administrators group.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure the system to include only administrator groups or accounts that are responsible for the system in the local Administrators group.
For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group.
Remove any standard user accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3(4)
800-53R5	AC-3(4)
CAT	I
CCI	CCI-002165
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSF	PR.AC-4
CSF	PR.PT-3
CSF2.0	PR.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.IR-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

ISO-27001-2022	A.5.15
ISO-27001-2022	A.5.33
ISO-27001-2022	A.8.3
ISO-27001-2022	A.8.18
ISO-27001-2022	A.8.20
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3(4)
NESA	T4.2.1
NESA	T5.4.4
NESA	T5.4.5
NESA	T5.5.4
NESA	T5.6.1
NESA	T7.5.2
NESA	T7.5.3
NIAV2	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-253269r958702_rule
STIG-ID	WN11-00-000070
TBA-FIISB	31.1
VULN-ID	V-253269

Assets

lognpacific3286

```
'Finding: LogNPacific3286\Guest is a standard user account in the local Administrators group.
Finding: LogNPacific3286\SantiagoX86 is a standard user account in the local Administrators
 group.'
```

WN11-00-000130 - Software certificate installation files must be removed from Windows 11.

Info

Use of software certificates and their accompanying installation files for end users to access resources is less secure than the use of hardware-based certificates.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Remove any certificate installation files (*.p12 and *.pfx) found on a system.
Note: This does not apply to server-based applications that have a requirement for .p12 certificate files (e.g., Oracle Wallet Manager) or Adobe PreFlight certificate files.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253280r991589_rule
STIG-ID	WN11-00-000130
SWIFT-CSCV1	2.3
VULN-ID	V-253280

Assets

lognpacific3286

WN11-00-000140 - Inbound exceptions to the firewall on Windows 11 domain workstations must only allow authorized remote management hosts.

Info

Allowing inbound access to domain workstations from other systems may allow lateral movement across systems if credentials are compromised. Limiting inbound connections only from authorized remote management systems will help limit this exposure.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure firewall exceptions to inbound connections on domain workstations to include only authorized remote management hosts.
Configure only inbound connection exceptions for authorized remote management hosts.
Computer Configuration >> Windows Settings >> Security Settings >> Windows Defender Firewall with Advanced Security >> Windows Defender Firewall with Advanced Security >> Inbound Rules (this link will be in the right pane)
For any inbound rules that allow connections, configure the Scope for Remote IP address to those of authorized remote management hosts. This may be defined as an IP address, subnet or range. Apply the rule to all firewall profiles.
If a third-party firewall is used, configure inbound exceptions to only include authorized remote management hosts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253282r991593_rule
STIG-ID	WN11-00-000140
SWIFT-CSCV1	2.3
VULN-ID	V-253282

```
 'DisplayName : Wi-Fi Direct Spooler Use (In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - IPv6 (IPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Delivery Optimization (UDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Advertisement (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Dynamic Host Configuration Protocol (DHCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery for Teredo (SSDP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Wi-Fi Direct Scan Service Use (In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD Events-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)
Enabled     : True
Direction   : Inbound

DisplayName : Remote Assistance (DCOM-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (WSD EventsSecure-In)
Enabled     : True
Direction   : Inbound

DisplayName : Remote Assistance (RA Server TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Network Discovery (UPnP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Microsoft Media Foundation Network Source IN [UDP 5004-5009]
Enabled     : True
Direction   : Inbound
```

```
DisplayName : Delivery Optimization (TCP-In)
Enabled     : True
Direction   : Inbound

DisplayName : Core Networking - Router Solicitation (ICMPv6-In)
Enabled     : True
Direction [...]
```

WN11-00-000190 - Orphaned security identifiers (SIDs) must be removed from user rights on Windows 11.

Info

Accounts or groups given rights on a system may show up as unresolved SIDs for various reasons including deletion of the accounts or groups. If the account or group objects are reanimated, there is a potential they may still have rights no longer intended. Valid domain accounts or groups may also show up as unresolved SIDs if a connection to the domain cannot be established for some reason.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Remove any unresolved SIDs found in User Rights assignments and determined to not be for currently valid accounts or groups by removing the accounts or groups from the appropriate group policy.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253290r991589_rule
STIG-ID	WN11-00-000190
SWIFT-CSCV1	2.3
VULN-ID	V-253290

Assets

lognpacific3286

WN11-00-000230 - The system must notify the user when a Bluetooth device attempts to connect.

Info

If not configured properly, Bluetooth may allow rogue devices to communicate with a system. If a rogue device is paired with a system, there is potential for sensitive information to be compromised.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure Bluetooth to notify users if devices attempt to connect.
View Bluetooth Settings.
Ensure 'Alert me when a new Bluetooth device wants to connect' is checked.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253293r991589_rule
STIG-ID	WN11-00-000230
SWIFT-CSCV1	2.3
VULN-ID	V-253293

Assets

lognpacific3286

```
Non-compliant items:
  HKU\S-1-5-21-108538807-2850267539-2289239689-500\Software\Microsoft\BluetoothAuthenticationAgent
 - 2
```

WN11-00-000240 - Administrative accounts must not be used with applications that access the internet, such as web browsers, or with potential internet sources, such as email.

Info

Using applications that access the internet or have potential internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while running as a privileged user, the entire system could be compromised. Web browsers and email are common attack vectors for introducing malicious code and must not be run with an administrative account.
Since administrative accounts may generally change or work around technical restrictions for running a web browser or other applications, it is essential that policy requires administrative accounts to not access the internet or use applications, such as email.
The policy must define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.
Technical means such as application allowlisting can be used to enforce the policy to ensure compliance.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Establish and enforce a policy that prohibits administrative accounts from using applications that access the internet, such as web browsers, or with potential internet sources, such as email. Define specific exceptions for local service administration. These exceptions may include HTTP(S)-based tools that are used for the administration of the local system, services, or attached devices.
Implement technical measures where feasible such as removal of applications or use of application allowlisting to restrict the use of applications that can access the internet.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-53	CM-6b.
800-53R5	CM-6b.
CAT	I
CCI	CCI-000366
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	PR.PS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ITSG-33	CM-6b.
NESA	T3.2.1
RULE-ID	SV-253294r991589_rule
STIG-ID	WN11-00-000240

SWIFT-CSCV1	2.3
VULN-ID	V-253294

Assets

lognpacific3286

WN11-00-000250 - Windows 11 nonpersistent VM sessions must not exceed 24 hours.

Info

For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshed upon logoff, the organization must enforce that sessions be terminated within 24 hours. This would ensure any data stored on the VM that is not encrypted or covered by Credential Guard is deleted.
NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Set nonpersistent VM sessions to not exceed 24 hours.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53R5	SC-28
CAT	II
CCI	CCI-001199
CN-L3	8.1.4.7(b)
CN-L3	8.1.4.8(b)
CSF	PR.DS-1
CSF2.0	PR.DS-01
DISA_BENCHMARK	Microsoft_Windows_11_STIG
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iv)
HIPAA	164.312(e)(2)(ii)
ISO-27001-2022	A.5.10
ISO-27001-2022	A.5.33
ITSG-33	SC-28
ITSG-33	SC-28a.
PCI-DSSV3.2.1	3.4
PCI-DSSV4.0	3.3.2
PCI-DSSV4.0	3.5.1
QCSC-V1	5.2.2

QCSC-V1	6.2
RULE-ID	SV-253295r958552_rule
STIG-ID	WN11-00-000250
VULN-ID	V-253295

Assets

lognpacific3286