

Tenable Vulnerability Management Report

Tenable Vulnerability Management

Wed, 14 May 2025 04:54:05 UTC

Table Of Contents

Audits FAILED.....	12
•WN19-00-000020 - Windows Server 2019 passwords for the built-in Administrator account must be changed at least every 60 days.....	13
•WN19-00-000140 - Windows Server 2019 permissions for the system drive root directory (usually C:\) must conform to minimum requirements.....	15
•WN19-00-000280 - Windows Server 2019 must have a host-based firewall installed and enabled.....	17
•WN19-00-000390 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol disabled on the SMB server.....	19
•WN19-00-000400 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol disabled on the SMB client.....	21
•WN19-AC-000010 - Windows Server 2019 account lockout duration must be configured to 15 minutes or greater.....	23
•WN19-AC-000020 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less.....	25
•WN19-AC-000030 - Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.....	27
•WN19-AC-000040 - Windows Server 2019 password history must be configured to 24 passwords remembered.....	29
•WN19-AC-000060 - Windows Server 2019 minimum password age must be configured to at least one day.....	31
•WN19-AC-000070 - Windows Server 2019 minimum password length must be configured to 14 characters.....	33
•WN19-AU-000080 - Windows Server 2019 must be configured to audit Account Logon - Credential Validation failures.....	35
•WN19-AU-000140 - Windows Server 2019 must be configured to audit Detailed Tracking - Process Creation successes.....	37
•WN19-AU-000170 - Windows Server 2019 must be configured to audit Logon/Logoff - Group Membership successes.....	40
•WN19-AU-000240 - Windows Server 2019 must be configured to audit Object Access - Removable Storage successes.....	42
•WN19-AU-000250 - Windows Server 2019 must be configured to audit Object Access - Removable Storage failures.....	44
•WN19-AU-000290 - Windows Server 2019 must be configured to audit Policy Change - Authorization Policy Change successes.....	46
•WN19-AU-000300 - Windows Server 2019 must be configured to audit Privilege Use - Sensitive Privilege Use successes.....	49
•WN19-AU-000310 - Windows Server 2019 must be configured to audit Privilege Use - Sensitive Privilege Use failures.....	52
•WN19-AU-000320 - Windows Server 2019 must be configured to audit System - IPsec Driver successes.....	55
•WN19-AU-000330 - Windows Server 2019 must be configured to audit System - IPsec Driver failures.....	58
•WN19-CC-000010 - Windows Server 2019 must prevent the display of slide shows on the lock screen.....	61
•WN19-CC-000020 - Windows Server 2019 must have WDigest Authentication disabled.....	63
•WN19-CC-000030 - Windows Server 2019 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.....	65
•WN19-CC-000040 - Windows Server 2019 source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.....	67
•WN19-CC-000050 - Windows Server 2019 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.....	69
•WN19-CC-000060 - Windows Server 2019 must be configured to ignore NetBIOS name release requests except from WINS servers.....	71
•WN19-CC-000070 - Windows Server 2019 insecure logons to an SMB server must be disabled.....	73
•WN19-CC-000080 - Windows Server 2019 hardened Universal Naming Convention (UNC) paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.....	74

●WN19-CC-000090 - Windows Server 2019 command line data must be included in process creation events.....	76
●WN19-CC-000100 - Windows Server 2019 must be configured to enable Remote host allows delegation of non-exportable credentials.....	78
●WN19-CC-000140 - Windows Server 2019 group policy objects must be reprocessed even if they have not changed.....	80
●WN19-CC-000150 - Windows Server 2019 downloading print driver packages over HTTP must be turned off.....	82
●WN19-CC-000160 - Windows Server 2019 printing over HTTP must be turned off.....	84
●WN19-CC-000170 - Windows Server 2019 network selection user interface (UI) must not be displayed on the logon screen.....	86
●WN19-CC-000180 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (on battery).....	88
●WN19-CC-000190 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (plugged in).....	90
●WN19-CC-000200 - Windows Server 2019 Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.....	92
●WN19-CC-000210 - Windows Server 2019 Autoplay must be turned off for non-volume devices.....	94
●WN19-CC-000220 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands.....	95
●WN19-CC-000230 - Windows Server 2019 AutoPlay must be disabled for all drives.....	97
●WN19-CC-000240 - Windows Server 2019 administrator accounts must not be enumerated during elevation.....	99
●WN19-CC-000250 - Windows Server 2019 Telemetry must be configured to Security or Basic.....	100
●WN19-CC-000260 - Windows Server 2019 Windows Update must not obtain updates from other PCs on the Internet.....	102
●WN19-CC-000270 - Windows Server 2019 Application event log size must be configured to 32768 KB or greater.....	104
●WN19-CC-000280 - Windows Server 2019 Security event log size must be configured to 196608 KB or greater.....	105
●WN19-CC-000290 - Windows Server 2019 System event log size must be configured to 32768 KB or greater....	106
●WN19-CC-000300 - Windows Server 2019 Windows Defender SmartScreen must be enabled.....	107
●WN19-CC-000340 - Windows Server 2019 must not save passwords in the Remote Desktop Client.....	109
●WN19-CC-000350 - Windows Server 2019 Remote Desktop Services must prevent drive redirection.....	110
●WN19-CC-000360 - Windows Server 2019 Remote Desktop Services must always prompt a client for passwords upon connection.....	111
●WN19-CC-000370 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications.....	112
●WN19-CC-000380 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High Level.....	114
●WN19-CC-000390 - Windows Server 2019 must prevent attachments from being downloaded from RSS feeds.....	116
●WN19-CC-000410 - Windows Server 2019 must prevent Indexing of encrypted files.....	117
●WN19-CC-000420 - Windows Server 2019 must prevent users from changing installation options.....	119
●WN19-CC-000430 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option.....	121
●WN19-CC-000460 - Windows Server 2019 PowerShell script block logging must be enabled.....	123
●WN19-CC-000470 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication.....	125
●WN19-CC-000480 - Windows Server 2019 Windows Remote Management (WinRM) client must not allow unencrypted traffic.....	126
●WN19-CC-000490 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Digest authentication.....	128
●WN19-CC-000500 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication.....	129

●WN19-CC-000510 - Windows Server 2019 Windows Remote Management (WinRM) service must not allow unencrypted traffic.....	130
●WN19-CC-000520 - Windows Server 2019 Windows Remote Management (WinRM) service must not store RunAs credentials.....	132
●WN19-CC-000530 - Windows Server 2019 must have PowerShell Transcription enabled.....	133
●WN19-MS-000040 - Windows Server 2019 must restrict unauthenticated Remote Procedure Call (RPC) clients from connecting to the RPC server on domain-joined member servers and standalone or nondomain-joined systems.....	135
●WN19-MS-000060 - Windows Server 2019 must restrict remote calls to the Security Account Manager (SAM) to Administrators on domain-joined member servers and standalone or nondomain-joined systems.....	137
●WN19-MS-000070 - Windows Server 2019 'Access this computer from the network' user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems.....	139
●WN19-MS-000080 - Windows Server 2019 'Deny access to this computer from the network' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems.....	141
●WN19-MS-000090 - Windows Server 2019 'Deny log on as a batch job' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.....	143
●WN19-MS-000110 - Windows Server 2019 'Deny log on locally' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.....	145
●WN19-MS-000120 - Windows Server 2019 'Deny log on through Remote Desktop Services' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and all local accounts and from unauthenticated access on all systems.....	147
●WN19-PK-000010 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store.....	149
●WN19-PK-000020 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems.....	151
●WN19-PK-000030 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems.....	153
●WN19-SO-000040 - Windows Server 2019 built-in guest account must be renamed.....	155
●WN19-SO-000050 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings.....	156
●WN19-SO-000120 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.....	158
●WN19-SO-000130 - Windows Server 2019 required legal notice must be configured to display before console logon.....	160
●WN19-SO-000140 - Windows Server 2019 title for legal banner dialog box must be configured with the appropriate text.....	162
●WN19-SO-000150 - Windows Server 2019 Smart Card removal option must be configured to Force Logoff or Lock Workstation.....	164
●WN19-SO-000160 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.....	165
●WN19-SO-000190 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.....	168
●WN19-SO-000200 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.....	171
●WN19-SO-000230 - Windows Server 2019 must not allow anonymous enumeration of shares.....	174
●WN19-SO-000260 - Windows Server 2019 services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.....	175
●WN19-SO-000270 - Windows Server 2019 must prevent NTLM from falling back to a Null session.....	177
●WN19-SO-000280 - Windows Server 2019 must prevent PKU2U authentication using online identities.....	178
●WN19-SO-000290 - Windows Server 2019 Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.....	179

•WN19-SO-000310 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM.....	181
•WN19-SO-000330 - Windows Server 2019 session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.....	183
•WN19-SO-000340 - Windows Server 2019 session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.....	185
•WN19-SO-000350 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer.....	187
•WN19-SO-000360 - Windows Server 2019 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.....	189
•WN19-SO-000380 - Windows Server 2019 User Account Control approval mode for the built-in Administrator must be enabled.....	191
•WN19-SO-000400 - Windows Server 2019 User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.....	192
•WN19-SO-000410 - Windows Server 2019 User Account Control must automatically deny standard user requests for elevation.....	193
•WN19-UR-000030 - Windows Server 2019 Allow log on locally user right must only be assigned to the Administrators group.....	194
•WN19-UR-000040 - Windows Server 2019 Back up files and directories user right must only be assigned to the Administrators group.....	196
•WN19-UR-000140 - Windows Server 2019 Increase scheduling priority: user right must only be assigned to the Administrators group.....	198
•WN19-UR-000210 - Windows Server 2019 Restore files and directories user right must only be assigned to the Administrators group.....	200

Audits SKIPPED..... 202

Audits PASSED..... 203

•DISA_Microsoft_Windows_Server_2019_STIG_v3r4.audit from DISA Microsoft Windows Server 2019 STIG v3r4.....	204
•WN19-00-000040 - Windows Server 2019 members of the Backup Operators group must have separate accounts for backup duties and normal operational tasks.....	205
•WN19-00-000060 - Windows Server 2019 manually managed application account passwords must be changed at least annually or when a system administrator with knowledge of the password leaves the organization.....	207
•WN19-00-000090 - Windows Server 2019 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.....	209
•WN19-00-000100 - Windows Server 2019 must be maintained at a supported servicing level.....	211
•WN19-00-000130 - Windows Server 2019 local volumes must use a format that supports NTFS attributes.....	212
•WN19-00-000150 - Windows Server 2019 permissions for program file directories must conform to minimum requirements.....	214
•WN19-00-000160 - Windows Server 2019 permissions for the Windows installation directory must conform to minimum requirements.....	217
•WN19-00-000170 - Windows Server 2019 default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.....	220
•WN19-00-000200 - Windows Server 2019 accounts must require passwords.....	223
•WN19-00-000210 - Windows Server 2019 passwords must be configured to expire.....	225
•WN19-00-000230 - Windows Server 2019 non-system-created file shares must limit access to groups that require it.....	227
•WN19-00-000320 - Windows Server 2019 must not have the Fax Server role installed.....	228
•WN19-00-000330 - Windows Server 2019 must not have the Microsoft FTP service installed unless required by the organization.....	230
•WN19-00-000340 - Windows Server 2019 must not have the Peer Name Resolution Protocol installed.....	232
•WN19-00-000350 - Windows Server 2019 must not have Simple TCP/IP Services installed.....	234
•WN19-00-000360 - Windows Server 2019 must not have the Telnet Client installed.....	236
•WN19-00-000370 - Windows Server 2019 must not have the TFTP Client installed.....	238

●WN19-00-000380 - Windows Server 2019 must not have the Server Message Block (SMB) v1 protocol installed.....	240
●WN19-00-000410 - Windows Server 2019 must not have Windows PowerShell 2.0 installed.....	242
●WN19-00-000440 - The Windows Server 2019 time service must synchronize with an appropriate DOD time source.....	244
●WN19-00-000460 - Windows Server 2019 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.....	246
●WN19-00-000470 - Windows Server 2019 must have Secure Boot enabled.....	247
●WN19-AC-000050 - Windows Server 2019 maximum password age must be configured to 60 days or less.....	248
●WN19-AC-000080 - Windows Server 2019 must have the built-in Windows password complexity policy enabled.....	250
●WN19-AC-000090 - Windows Server 2019 reversible password encryption must be disabled.....	252
●WN19-AU-000030 - Windows Server 2019 permissions for the Application event log must prevent access by non-privileged accounts.....	254
●WN19-AU-000040 - Windows Server 2019 permissions for the Security event log must prevent access by non-privileged accounts.....	256
●WN19-AU-000050 - Windows Server 2019 permissions for the System event log must prevent access by non-privileged accounts.....	258
●WN19-AU-000060 - Windows Server 2019 Event Viewer must be protected from unauthorized modification and deletion.....	260
●WN19-AU-000070 - Windows Server 2019 must be configured to audit Account Logon - Credential Validation successes.....	262
●WN19-AU-000090 - Windows Server 2019 must be configured to audit Account Management - Other Account Management Events successes.....	264
●WN19-AU-000100 - Windows Server 2019 must be configured to audit Account Management - Security Group Management successes.....	267
●WN19-AU-000110 - Windows Server 2019 must be configured to audit Account Management - User Account Management successes.....	270
●WN19-AU-000120 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures.....	273
●WN19-AU-000130 - Windows Server 2019 must be configured to audit Detailed Tracking - Plug and Play Events successes.....	276
●WN19-AU-000160 - Windows Server 2019 must be configured to audit Logon/Logoff - Account Lockout failures.....	278
●WN19-AU-000180 - Windows Server 2019 must be configured to audit logoff successes.....	281
●WN19-AU-000190 - Windows Server 2019 must be configured to audit logon successes.....	284
●WN19-AU-000200 - Windows Server 2019 must be configured to audit logon failures.....	287
●WN19-AU-000210 - Windows Server 2019 must be configured to audit Logon/Logoff - Special Logon successes.....	290
●WN19-AU-000220 - Windows Server 2019 must be configured to audit Object Access - Other Object Access Events successes.....	292
●WN19-AU-000230 - Windows Server 2019 must be configured to audit Object Access - Other Object Access Events failures.....	294
●WN19-AU-000260 - Windows Server 2019 must be configured to audit Policy Change - Audit Policy Change successes.....	296
●WN19-AU-000270 - Windows Server 2019 must be configured to audit Policy Change - Audit Policy Change failures.....	299
●WN19-AU-000280 - Windows Server 2019 must be configured to audit Policy Change - Authentication Policy Change successes.....	302
●WN19-AU-000340 - Windows Server 2019 must be configured to audit System - Other System Events successes.....	305
●WN19-AU-000350 - Windows Server 2019 must be configured to audit System - Other System Events failures.....	308

●WN19-AU-000360 - Windows Server 2019 must be configured to audit System - Security State Change successes.....	311
●WN19-AU-000370 - Windows Server 2019 must be configured to audit System - Security System Extension successes.....	314
●WN19-AU-000380 - Windows Server 2019 must be configured to audit System - System Integrity successes.....	317
●WN19-AU-000390 - Windows Server 2019 must be configured to audit System - System Integrity failures.....	320
●WN19-CC-000110 - Windows Server 2019 virtualization-based security must be enabled with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.....	323
●WN19-CC-000130 - Windows Server 2019 Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.....	325
●WN19-CC-000310 - Windows Server 2019 Explorer Data Execution Prevention must be enabled.....	327
●WN19-CC-000320 - Windows Server 2019 Turning off File Explorer heap termination on corruption must be disabled.....	328
●WN19-CC-000330 - Windows Server 2019 File Explorer shell protocol must run in protected mode.....	330
●WN19-CC-000400 - Windows Server 2019 must disable Basic authentication for RSS feeds over HTTP.....	331
●WN19-CC-000440 - Windows Server 2019 users must be notified if a web-based program attempts to install software.....	333
●WN19-CC-000450 - Windows Server 2019 must disable automatically signing in the last interactive user after a system-initiated restart.....	335
●WN19-DC-000010 - Windows Server 2019 must only allow administrators responsible for the domain controller to have Administrator rights on the system.....	337
●WN19-DC-000020 - Windows Server 2019 Kerberos user logon restrictions must be enforced.....	339
●WN19-DC-000030 - Windows Server 2019 Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.....	341
●WN19-DC-000040 - Windows Server 2019 Kerberos user ticket lifetime must be limited to 10 hours or less.....	343
●WN19-DC-000050 - Windows Server 2019 Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.....	345
●WN19-DC-000060 - Windows Server 2019 computer clock synchronization tolerance must be limited to five minutes or less.....	347
●WN19-DC-000070 - Windows Server 2019 permissions on the Active Directory data files must only allow System and Administrators access.....	349
●WN19-DC-000080 - Windows Server 2019 Active Directory SYSVOL directory must have the proper access control permissions.....	351
●WN19-DC-000090 - Windows Server 2019 Active Directory Group Policy objects must have proper access control permissions.....	353
●WN19-DC-000100 - Windows Server 2019 Active Directory Domain Controllers Organizational Unit (OU) object must have the proper access control permissions.....	355
●WN19-DC-000110 - Windows Server 2019 organization created Active Directory Organizational Unit (OU) objects must have proper access control permissions.....	358
●WN19-DC-000120 - Windows Server 2019 data files owned by users must be on a different logical partition from the directory server data files.....	361
●WN19-DC-000130 - Windows Server 2019 domain controllers must run on a machine dedicated to that function.....	362
●WN19-DC-000140 - Windows Server 2019 must use separate, NSA-approved (Type 1) cryptography to protect the directory data in transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.....	364
●WN19-DC-000150 - Windows Server 2019 directory data (outside the root DSE) of a non-public directory must be configured to prevent anonymous access.....	366
●WN19-DC-000160 - Windows Server 2019 directory service must be configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity.....	368
●WN19-DC-000170 - Windows Server 2019 Active Directory Group Policy objects must be configured with proper audit settings.....	370
●WN19-DC-000180 - Windows Server 2019 Active Directory Domain object must be configured with proper audit settings.....	374

●WN19-DC-000190 - Windows Server 2019 Active Directory Infrastructure object must be configured with proper audit settings.....	378
●WN19-DC-000200 - Windows Server 2019 Active Directory Domain Controllers Organizational Unit (OU) object must be configured with proper audit settings.....	382
●WN19-DC-000210 - Windows Server 2019 Active Directory AdminSDHolder object must be configured with proper audit settings.....	386
●WN19-DC-000220 - Windows Server 2019 Active Directory RID Manager\$ object must be configured with proper audit settings.....	390
●WN19-DC-000230 - Windows Server 2019 must be configured to audit Account Management - Computer Account Management successes.....	394
●WN19-DC-000240 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access successes.....	397
●WN19-DC-000250 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access failures.....	400
●WN19-DC-000260 - Windows Server 2019 must be configured to audit DS Access - Directory Service Changes successes.....	403
●WN19-DC-000280 - Windows Server 2019 domain controllers must have a PKI server certificate.....	406
●WN19-DC-000290 - Windows Server 2019 domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority (ECA).....	408
●WN19-DC-000300 - Windows Server 2019 PKI certificates associated with user accounts must be issued by a DoD PKI or an approved External Certificate Authority (ECA).....	410
●WN19-DC-000310 - Windows Server 2019 Active Directory user accounts, including administrators, must be configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT) for user authentication.....	412
●WN19-DC-000320 - Windows Server 2019 domain controllers must require LDAP access signing.....	415
●WN19-DC-000330 - Windows Server 2019 domain controllers must be configured to allow reset of machine account passwords.....	418
●WN19-DC-000340 - Windows Server 2019 Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.....	420
●WN19-DC-000350 - Windows Server 2019 Add workstations to domain user right must only be assigned to the Administrators group on domain controllers.....	422
●WN19-DC-000360 - Windows Server 2019 Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group on domain controllers.....	424
●WN19-DC-000370 - Windows Server 2019 Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.....	426
●WN19-DC-000380 - Windows Server 2019 Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.....	428
●WN19-DC-000390 - Windows Server 2019 Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.....	430
●WN19-DC-000391 - Windows Server 2019 must be configured for certificate-based authentication for domain controllers.....	432
●WN19-DC-000400 - Windows Server 2019 Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.....	434
●WN19-DC-000401 - Windows Server 2019 must be configured for named-based strong mappings for certificates.....	436
●WN19-DC-000410 - Windows Server 2019 Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.....	438
●WN19-DC-000420 - Windows Server 2019 Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.....	440
●WN19-DC-000430 - The password for the krbtgt account on a domain must be reset at least every 180 days.....	442
●WN19-MS-000020 - Windows Server 2019 local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain-joined member servers.....	444
●WN19-MS-000030 - Windows Server 2019 local users on domain-joined member servers must not be enumerated.....	445

●WN19-MS-000050 - Windows Server 2019 must limit the caching of logon credentials to four or less on domain-joined member servers.....	447
●WN19-MS-000100 - Windows Server 2019 'Deny log on as a service' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts. No other groups or accounts must be assigned this right.....	449
●WN19-MS-000130 - Windows Server 2019 'Enable computer and user accounts to be trusted for delegation' user right must not be assigned to any groups or accounts on domain-joined member servers and standalone or nondomain-joined systems.....	451
●WN19-MS-000140 - Windows Server 2019 must be running Credential Guard on domain-joined member servers.....	453
●WN19-SO-000010 - Windows Server 2019 must have the built-in guest account disabled.....	455
●WN19-SO-000020 - Windows Server 2019 must prevent local accounts with blank passwords from being used from the network.....	457
●WN19-SO-000030 - Windows Server 2019 built-in administrator account must be renamed.....	459
●WN19-SO-000060 - Windows Server 2019 setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.....	460
●WN19-SO-000070 - Windows Server 2019 setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.....	463
●WN19-SO-000080 - Windows Server 2019 setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.....	466
●WN19-SO-000090 - Windows Server 2019 computer account password must not be prevented from being reset.....	469
●WN19-SO-000100 - Windows Server 2019 maximum age for machine account passwords must be configured to 30 days or less.....	471
●WN19-SO-000110 - Windows Server 2019 must be configured to require a strong session key.....	473
●WN19-SO-000170 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.....	476
●WN19-SO-000180 - Windows Server 2019 unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.....	479
●WN19-SO-000210 - Windows Server 2019 must not allow anonymous SID/Name translation.....	481
●WN19-SO-000220 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts.....	482
●WN19-SO-000240 - Windows Server 2019 must be configured to prevent anonymous users from having the same permissions as the Everyone group.....	483
●WN19-SO-000250 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares.....	484
●WN19-SO-000300 - Windows Server 2019 must be configured to prevent the storage of the LAN Manager hash of passwords.....	485
●WN19-SO-000320 - Windows Server 2019 must be configured to at least negotiate signing for LDAP client signing.....	487
●WN19-SO-000370 - Windows Server 2019 default permissions of global system objects must be strengthened.....	488
●WN19-SO-000390 - Windows Server 2019 UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.....	490
●WN19-SO-000420 - Windows Server 2019 User Account Control must be configured to detect application installations and prompt for elevation.....	491
●WN19-SO-000430 - Windows Server 2019 User Account Control (UAC) must only elevate UIAccess applications that are installed in secure locations.....	492
●WN19-SO-000440 - Windows Server 2019 User Account Control must run all administrators in Admin Approval Mode, enabling UAC.....	493
●WN19-SO-000450 - Windows Server 2019 User Account Control (UAC) must virtualize file and registry write failures to per-user locations.....	494
●WN19-UC-000010 - Windows Server 2019 must preserve zone information when saving attachments.....	495
●WN19-UR-000010 - Windows Server 2019 Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.....	497

●WN19-UR-000020 - Windows Server 2019 Act as part of the operating system user right must not be assigned to any groups or accounts.....	499
●WN19-UR-000050 - Windows Server 2019 Create a pagefile user right must only be assigned to the Administrators group.....	501
●WN19-UR-000060 - Windows Server 2019 Create a token object user right must not be assigned to any groups or accounts.....	503
●WN19-UR-000070 - Windows Server 2019 Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.....	505
●WN19-UR-000080 - Windows Server 2019 Create permanent shared objects user right must not be assigned to any groups or accounts.....	507
●WN19-UR-000090 - Windows Server 2019 Create symbolic links user right must only be assigned to the Administrators group.....	509
●WN19-UR-000100 - Windows Server 2019 Debug programs: user right must only be assigned to the Administrators group.....	511
●WN19-UR-000110 - Windows Server 2019 Force shutdown from a remote system user right must only be assigned to the Administrators group.....	513
●WN19-UR-000120 - Windows Server 2019 Generate security audits user right must only be assigned to Local Service and Network Service.....	515
●WN19-UR-000130 - Windows Server 2019 Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.....	517
●WN19-UR-000150 - Windows Server 2019 Load and unload device drivers user right must only be assigned to the Administrators group.....	519
●WN19-UR-000160 - Windows Server 2019 Lock pages in memory user right must not be assigned to any groups or accounts.....	521
●WN19-UR-000170 - Windows Server 2019 Manage auditing and security log user right must only be assigned to the Administrators group.....	523
●WN19-UR-000180 - Windows Server 2019 Modify firmware environment values user right must only be assigned to the Administrators group.....	526
●WN19-UR-000190 - Windows Server 2019 Perform volume maintenance tasks user right must only be assigned to the Administrators group.....	528
●WN19-UR-000200 - Windows Server 2019 Profile single process user right must only be assigned to the Administrators group.....	530
●WN19-UR-000220 - Windows Server 2019 Take ownership of files or other objects user right must only be assigned to the Administrators group.....	532

Audits INFO,WARNING,ERROR.....534

●WN19-00-000010 - Windows Server 2019 users with Administrative privileges must have separate accounts for administrative duties and normal operational tasks.....	535
●WN19-00-000030 - Windows Server 2019 administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.....	536
●WN19-00-000050 - Windows Server 2019 manually managed application account passwords must be at least 14 characters in length.....	538
●WN19-00-000070 - Windows Server 2019 shared user accounts must not be permitted.....	540
●WN19-00-000080 - Windows Server 2019 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.....	542
●WN19-00-000110 - Windows Server 2019 must use an anti-virus program.....	544
●WN19-00-000120 - Windows Server 2019 must have a host-based intrusion detection or prevention system.....	546
●WN19-00-000180 - Windows Server 2019 non-administrative accounts or groups must only have print permissions on printer shares.....	548
●WN19-00-000190 - Windows Server 2019 outdated or unused accounts must be removed or disabled.....	550
●WN19-00-000220 - Windows Server 2019 system files must be monitored for unauthorized changes.....	552
●WN19-00-000240 - Windows Server 2019 must have software certificate installation files removed.....	554
●WN19-00-000250 - Windows Server 2019 systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.....	555

●WN19-00-000260 - Windows Server 2019 must implement protection methods such as TLS, encrypted VPNs, or IPsec if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.....	557
●WN19-00-000270 - Windows Server 2019 must have the roles and features required by the system documented.....	560
●WN19-00-000290 - Windows Server 2019 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where Endpoint Security Solution (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).....	562
●WN19-00-000300 - Windows Server 2019 must automatically remove or disable temporary user accounts after 72 hours.....	564
●WN19-00-000310 - Windows Server 2019 must automatically remove or disable emergency accounts after the crisis is resolved or within 72 hours.....	566
●WN19-00-000420 - Windows Server 2019 FTP servers must be configured to prevent anonymous logons.....	568
●WN19-00-000430 - Windows Server 2019 FTP servers must be configured to prevent access to the system drive.....	570
●WN19-00-000450 - Windows Server 2019 must have orphaned security identifiers (SIDs) removed from user rights.....	571
●WN19-AU-000010 - Windows Server 2019 audit records must be backed up to a different system or media than the system being audited.....	573
●WN19-AU-000020 - Windows Server 2019 must, at a minimum, offload audit records of interconnected systems in real time and offload standalone or nondomain-joined systems weekly.....	574
●WN19-MS-000010 - Windows Server 2019 must only allow Administrators responsible for the member server or standalone or nondomain-joined system to have Administrator rights on the system.....	575

Audits FAILED

WN19-00-000020 - Windows Server 2019 passwords for the built-in Administrator account 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. The built-in Administrator account is not generally used and its password might not be changed as frequently as necessary. Changing the password for the built-in Administrator account 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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205657r1051065_rule
STIG-ID	WN19-00-000020
STIG-LEGACY	SV-103559
STIG-LEGACY	V-93473
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-205657

Assets

live-malware

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'
```


WN19-00-000140 - Windows Server 2019 permissions for the system drive root directory (usually C:) 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.

The default permissions are adequate when the Security Option 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (WN19-SO-000240).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Solution

Maintain the default permissions for the system drive's root directory and configure the Security Option 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (WN19-SO-000240).

Default Permissions C:\ Type - 'Allow' for all Inherited from - 'None' for all

Principal - Access - Applies to

SYSTEM - Full control - This folder, subfolders, and files Administrators - Full control - This folder, subfolders, and files

Users - Read & execute - This folder, subfolders, and files Users - Create folders/append data - This folder and subfolders

Users - Create files/write data - Subfolders only CREATOR OWNER - Full Control - Subfolders and files only

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205734r958702_rule
STIG-ID	WN19-00-000140
STIG-LEGACY	SV-103107
STIG-LEGACY	V-93019
TBA-FIISB	31.1
VULN-ID	V-205734

Assets

live-malware

```
'C:\ NT AUTHORITY\Authenticated Users:(AD)
  NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(M)
  NT AUTHORITY\SYSTEM:(OI)(CI)(F)
  BUILTIN\Administrators:(OI)(CI)(F)
  BUILTIN\Users:(OI)(CI)(RX)
  Mandatory Label\High Mandatory Level:(OI)(NP)(IO)(NW)
```

Successfully processed 1 files; Failed processing 0 files

STATUS: FAILED'

WN19-00-000280 - Windows Server 2019 must have a host-based firewall installed and enabled.

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_Server_2019_V3R4_STIG.zip

References

800-171	3.4.2
800-171R3	03.04.02a.
800-171R3	03.13.06
800-53	CA-3(5)
800-53	CM-6b.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000366
CCI	CCI-002080
CN-L3	8.1.10.6(d)
CSF	DE.AE-1
CSF	ID.AM-3
CSF	PR.IP-1
CSF2.0	DE.CM-09
CSF2.0	ID.AM-03
CSF2.0	PR.DS-01
CSF2.0	PR.DS-02
CSF2.0	PR.DS-10
CSF2.0	PR.PS-01
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO-27001-2022	A.5.14

ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.21
ITSG-33	CA-3
ITSG-33	CM-6b.
NESA	M1.3.5
NESA	M1.3.7
NESA	T3.2.1
NESA	T5.4.2
QCSC-V1	4.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
RULE-ID	SV-214936r991589_rule
STIG-ID	WN19-00-000280
STIG-LEGACY	SV-103657
STIG-LEGACY	V-93571
SWIFT-CSCV1	2.3
SWIFT-CSCV1	2.5
VULN-ID	V-214936

Assets

live-malware

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

```

WN19-00-000390 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol 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.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> MS Security Guide >> 'Configure SMBv1 Server' to 'Disabled'.

The system must be restarted for the change to take effect.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package.

'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205683r958478_rule
STIG-ID	WN19-00-000390

STIG-LEGACY	SV-103479
-------------	-----------

STIG-LEGACY	V-93393
-------------	---------

SWIFT-CSCV1	2.3
-------------	-----

VULN-ID	V-205683
---------	----------

Assets

live-malware

NULL

WN19-00-000400 - Windows Server 2019 must have the Server Message Block (SMB) v1 protocol 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.

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'.

The system must be restarted for the changes to take effect.

This policy setting requires the installation of the SecGuide custom templates included with the STIG package.

'SecGuide.admx' and 'SecGuide.adml' must be copied to the \Windows\PolicyDefinitions and \Windows\PolicyDefinitions\en-US directories respectively.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205684r958478_rule

STIG-ID	WN19-00-000400
---------	----------------

STIG-LEGACY	SV-103481
-------------	-----------

STIG-LEGACY	V-93395
-------------	---------

SWIFT-CSCV1	2.3
-------------	-----

VULN-ID	V-205684
---------	----------

Assets

live-malware

NULL

WN19-AC-000010 - Windows Server 2019 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 period 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_Server_2019_V3R4_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	Windows_Server_2019_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-205795r958736_rule
STIG-ID	WN19-AC-000010
STIG-LEGACY	SV-103233
STIG-LEGACY	V-93145
TBA-FIISB	36.2.4

TBA-FIISB	45.1.2
VULN-ID	V-205795

Assets

live-malware

10

WN19-AC-000020 - Windows Server 2019 must have the number of allowed bad logon attempts 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 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 fewer invalid logon attempts (excluding '0', which is unacceptable).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205629r958388_rule
STIG-ID	WN19-AC-000020
STIG-LEGACY	SV-103229
STIG-LEGACY	V-93141
TBA-FIISB	45.1.2

TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-205629

Assets

live-malware

10

WN19-AC-000030 - Windows Server 2019 must have the period of time before the bad logon counter is reset 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 period of time that must pass after failed logon attempts before the counter is reset to '0'. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.8
800-171R3	03.01.08a.
800-171R3	03.01.08b.
800-53	AC-7a.
800-53	AC-7b.
800-53R5	AC-7a.
800-53R5	AC-7b.
CAT	II
CCI	CCI-000044
CCI	CCI-002238
CN-L3	7.1.2.7(f)
CN-L3	7.1.3.1(c)
CN-L3	8.1.4.1(b)
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-7a.
ITSG-33	AC-7b.
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6

PCI-DSSV3.2.1	8.1.7
PCI-DSSV4.0	8.3.4
RULE-ID	SV-205630r958388_rule
STIG-ID	WN19-AC-000030
STIG-LEGACY	SV-103231
STIG-LEGACY	V-93143
TBA-FIISB	36.2.4
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2
VULN-ID	V-205630

Assets

live-malware

10

WN19-AC-000040 - Windows Server 2019 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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205660r1000129_rule

STIG-ID	WN19-AC-000040
STIG-LEGACY	SV-103565
STIG-LEGACY	V-93479
SWIFT-CSCV1	4.1
VULN-ID	V-205660

Assets

live-malware

0

WN19-AC-000060 - Windows Server 2019 minimum password age must be configured to at least one 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_Server_2019_V3R4_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	Windows_Server_2019_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-205656r1051064_rule
STIG-ID	WN19-AC-000060
STIG-LEGACY	SV-103557
STIG-LEGACY	V-93471
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-205656

Assets

live-malware

0

WN19-AC-000070 - Windows Server 2019 minimum password length must be configured to 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_Server_2019_V3R4_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	Windows_Server_2019_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-205662r1051069_rule
STIG-ID	WN19-AC-000070
STIG-LEGACY	SV-103549
STIG-LEGACY	V-93463
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-205662

Assets

live-malware

0

WN19-AU-000080 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205833r991578_rule
STIG-ID	WN19-AU-000080
STIG-LEGACY	SV-103243
STIG-LEGACY	V-93155
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205833

Assets

live-malware

'success'

WN19-AU-000140 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205770r958732_rule
STIG-ID	WN19-AU-000140
STIG-LEGACY	SV-103179
STIG-LEGACY	V-93091
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205770

Assets

live-malware

'no auditing'

WN19-AU-000170 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205834r991578_rule
STIG-ID	WN19-AU-000170
STIG-LEGACY	SV-103247
STIG-LEGACY	V-93159
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205834

Assets

live-malware

'no auditing'

WN19-AU-000240 - Windows Server 2019 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.

Removable Storage auditing under Object Access 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_Server_2019_V3R4_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	Windows_Server_2019_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-205840r991583_rule
STIG-ID	WN19-AU-000240
STIG-LEGACY	SV-103255
STIG-LEGACY	V-93167
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205840

Assets

live-malware

'no auditing'

WN19-AU-000250 - Windows Server 2019 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.

Removable Storage auditing under Object Access 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_Server_2019_V3R4_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	Windows_Server_2019_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-205841r991583_rule
STIG-ID	WN19-AU-000250
STIG-LEGACY	SV-103257
STIG-LEGACY	V-93169
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205841

Assets

live-malware

'no auditing'

WN19-AU-000290 - Windows Server 2019 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'.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205774r958732_rule
STIG-ID	WN19-AU-000290
STIG-LEGACY	SV-103187
STIG-LEGACY	V-93099
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205774

Assets

live-malware

'no auditing'

WN19-AU-000300 - Windows Server 2019 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'.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)

CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4

NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205775r958732_rule
STIG-ID	WN19-AU-000300
STIG-LEGACY	SV-103189
STIG-LEGACY	V-93101
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205775

Assets

live-malware

'no auditing'

WN19-AU-000310 - Windows Server 2019 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'.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)

CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4

NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205776r958732_rule
STIG-ID	WN19-AU-000310
STIG-LEGACY	SV-103191
STIG-LEGACY	V-93103
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205776

Assets

live-malware

'no auditing'

WN19-AU-000320 - Windows Server 2019 must be configured to audit System - IPsec Driver 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.

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205777r958732_rule
STIG-ID	WN19-AU-000320
STIG-LEGACY	SV-103193
STIG-LEGACY	V-93105
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205777

Assets

live-malware

'no auditing'

WN19-AU-000330 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)

CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1

NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205778r958732_rule
STIG-ID	WN19-AU-000330
STIG-LEGACY	SV-103195
STIG-LEGACY	V-93107
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205778

Assets

live-malware

'no auditing'

WN19-CC-000010 - Windows Server 2019 must prevent the display of slide shows on the lock screen.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205686r958478_rule
STIG-ID	WN19-CC-000010
STIG-LEGACY	SV-103485
STIG-LEGACY	V-93399

SWIFT-CSCV1

2.3

VULN-ID

V-205686

Assets

live-malware

NULL

WN19-CC-000020 - Windows Server 2019 must have WDigest Authentication 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 Server 2019. 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'.
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_Server_2019_V3R4_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	Windows_Server_2019_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-205687r958478_rule
STIG-ID	WN19-CC-000020

STIG-LEGACY	SV-103487
-------------	-----------

STIG-LEGACY	V-93401
-------------	---------

SWIFT-CSCV1	2.3
-------------	-----

VULN-ID	V-205687
---------	----------

Assets

live-malware

NULL

WN19-CC-000030 - Windows Server 2019 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.

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 'Enabled' with 'Highest protection, source routing is completely disabled' selected.

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205858r991589_rule
STIG-ID	WN19-CC-000030
STIG-LEGACY	SV-103321
STIG-LEGACY	V-93233
SWIFT-CSCV1	2.3
VULN-ID	V-205858

Assets

live-malware

NULL

WN19-CC-000040 - Windows Server 2019 source routing must be configured to the highest protection level to prevent Internet Protocol (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 'Enabled' with 'Highest protection, source routing is completely disabled' selected.

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205859r991589_rule
STIG-ID	WN19-CC-000040
STIG-LEGACY	SV-103323
STIG-LEGACY	V-93235
SWIFT-CSCV1	2.3
VULN-ID	V-205859

Assets

live-malware

NULL

WN19-CC-000050 - Windows Server 2019 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 the 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_Server_2019_V3R4_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	Windows_Server_2019_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-205860r991589_rule
STIG-ID	WN19-CC-000050
STIG-LEGACY	SV-103325
STIG-LEGACY	V-93237
SWIFT-CSCV1	2.3
VULN-ID	V-205860

Assets

live-malware

NULL

WN19-CC-000060 - Windows Server 2019 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 server's 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_Server_2019_V3R4_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	Windows_Server_2019_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-205819r958902_rule
STIG-ID	WN19-CC-000060
STIG-LEGACY	SV-103627
STIG-LEGACY	V-93541

VULN-ID

V-205819

Assets

live-malware

NULL

WN19-CC-000070 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205861r991589_rule
STIG-ID	WN19-CC-000070
STIG-LEGACY	SV-103327
STIG-LEGACY	V-93239
SWIFT-CSCV1	2.3
VULN-ID	V-205861

Assets

live-malware

NULL

WN19-CC-000080 - Windows Server 2019 hardened Universal Naming Convention (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 UNC paths specified in hardened UNC paths before allowing access to them. This aids in preventing tampering with or spoofing of connections to these paths.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205862r991589_rule
STIG-ID	WN19-CC-000080
STIG-LEGACY	SV-103329
STIG-LEGACY	V-93241
SWIFT-CSCV1	2.3
VULN-ID	V-205862

Assets

live-malware

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'

WN19-CC-000090 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205638r958422_rule
STIG-ID	WN19-CC-000090
STIG-LEGACY	SV-103261
STIG-LEGACY	V-93173
SWIFT-CSCV1	6.4
VULN-ID	V-205638

Assets

live-malware

NULL

WN19-CC-000100 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205863r991589_rule
STIG-ID	WN19-CC-000100
STIG-LEGACY	SV-103331
STIG-LEGACY	V-93243
SWIFT-CSCV1	2.3
VULN-ID	V-205863

Assets

live-malware

NULL

WN19-CC-000140 - Windows Server 2019 group policy objects must be reprocessed even if they have not changed.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205866r991589_rule
STIG-ID	WN19-CC-000140
STIG-LEGACY	SV-103339
STIG-LEGACY	V-93251
SWIFT-CSCV1	2.3
VULN-ID	V-205866

Assets

live-malware

NULL

WN19-CC-000150 - Windows Server 2019 downloading print driver packages over HTTP must be turned off.

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 will prevent 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_Server_2019_V3R4_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	Windows_Server_2019_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-205688r958478_rule
STIG-ID	WN19-CC-000150

STIG-LEGACY	SV-103489
-------------	-----------

STIG-LEGACY	V-93403
-------------	---------

SWIFT-CSCV1	2.3
-------------	-----

VULN-ID	V-205688
---------	----------

Assets

live-malware

NULL

WN19-CC-000160 - Windows Server 2019 printing over HTTP must be turned off.

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 will prevent uncontrolled updates to the system.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205689r958478_rule
STIG-ID	WN19-CC-000160
STIG-LEGACY	SV-103491

STIG-LEGACY

V-93405

SWIFT-CSCV1

2.3

VULN-ID

V-205689

Assets

live-malware

NULL

WN19-CC-000170 - Windows Server 2019 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 in to 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_Server_2019_V3R4_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	Windows_Server_2019_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-205690r958478_rule
STIG-ID	WN19-CC-000170
STIG-LEGACY	SV-103493
STIG-LEGACY	V-93407

SWIFT-CSCV1

2.3

VULN-ID

V-205690

Assets

live-malware

NULL

WN19-CC-000180 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (on battery).

Info

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205867r991589_rule
STIG-ID	WN19-CC-000180
STIG-LEGACY	SV-103341
STIG-LEGACY	V-93253
SWIFT-CSCV1	2.3
VULN-ID	V-205867

Assets

live-malware

NULL

WN19-CC-000190 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (plugged in).

Info

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205868r991589_rule
STIG-ID	WN19-CC-000190
STIG-LEGACY	SV-103343
STIG-LEGACY	V-93255
SWIFT-CSCV1	2.3
VULN-ID	V-205868

Assets

live-malware

NULL

WN19-CC-000200 - Windows Server 2019 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 will prevent uncontrolled updates to the system.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205691r958478_rule
STIG-ID	WN19-CC-000200

STIG-LEGACY	SV-103495
-------------	-----------

STIG-LEGACY	V-93409
-------------	---------

SWIFT-CSCV1	2.3
-------------	-----

VULN-ID	V-205691
---------	----------

Assets

live-malware

NULL

WN19-CC-000210 - Windows Server 2019 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 into the drive. As a result, the setup file of programs or music on audio media may start. This setting will disable AutoPlay for non-volume devices, such as Media Transfer Protocol (MTP) devices.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205804r958804_rule
STIG-ID	WN19-CC-000210
STIG-LEGACY	SV-103459
STIG-LEGACY	V-93373
SWIFT-CSCV1	2.3
VULN-ID	V-205804

Assets

live-malware

NULL

WN19-CC-000220 - Windows Server 2019 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' with 'Do not execute any autorun commands' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205805r958804_rule
STIG-ID	WN19-CC-000220
STIG-LEGACY	SV-103461
STIG-LEGACY	V-93375
SWIFT-CSCV1	2.3
VULN-ID	V-205805

Assets

live-malware

NULL

WN19-CC-000230 - Windows Server 2019 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 media is inserted into the drive. As a result, the setup file of programs or music on audio media may start. By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives. Enabling this policy disables AutoPlay on all drives.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205806r958804_rule
STIG-ID	WN19-CC-000230
STIG-LEGACY	SV-103463
STIG-LEGACY	V-93377
SWIFT-CSCV1	2.3
VULN-ID	V-205806

Assets

live-malware

NULL

WN19-CC-000240 - Windows Server 2019 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_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205714r958518_rule
STIG-ID	WN19-CC-000240
STIG-LEGACY	SV-103603
STIG-LEGACY	V-93517
VULN-ID	V-205714

Assets

live-malware

NULL

WN19-CC-000250 - Windows Server 2019 Telemetry must be configured to Security or Basic.

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.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205869r991589_rule
STIG-ID	WN19-CC-000250
STIG-LEGACY	SV-103345
STIG-LEGACY	V-93257
SWIFT-CSCV1	2.3
VULN-ID	V-205869

Assets

live-malware

NULL

WN19-CC-000260 - Windows Server 2019 Windows Update must not obtain updates from other PCs on the Internet.

Info

Windows Update can 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_Server_2019_V3R4_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	Windows_Server_2019_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-205870r991589_rule
STIG-ID	WN19-CC-000260
STIG-LEGACY	SV-103347
STIG-LEGACY	V-93259
SWIFT-CSCV1	2.3
VULN-ID	V-205870

Assets

live-malware

NULL

WN19-CC-000270 - Windows Server 2019 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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205796r958752_rule
STIG-ID	WN19-CC-000270
STIG-LEGACY	SV-103265
STIG-LEGACY	V-93177
VULN-ID	V-205796

Assets

live-malware

NULL

WN19-CC-000280 - Windows Server 2019 Security event log size must be configured to 196608 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 '196608' or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205797r958752_rule
STIG-ID	WN19-CC-000280
STIG-LEGACY	SV-103267
STIG-LEGACY	V-93179
VULN-ID	V-205797

Assets

live-malware

NULL

WN19-CC-000290 - Windows Server 2019 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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205798r958752_rule
STIG-ID	WN19-CC-000290
STIG-LEGACY	SV-103269
STIG-LEGACY	V-93181
VULN-ID	V-205798

Assets

live-malware

NULL

WN19-CC-000300 - Windows Server 2019 Windows Defender SmartScreen must be enabled.

Info

Windows Defender SmartScreen helps protect systems from programs downloaded from the internet that may be malicious. Enabling SmartScreen can block potentially malicious programs or warn users.

Solution

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> File Explorer >> 'Configure Windows Defender SmartScreen' to 'Enabled' with either option 'Warn' or 'Warn and prevent bypass' selected.

Windows 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205692r958478_rule
STIG-ID	WN19-CC-000300
STIG-LEGACY	SV-103497

STIG-LEGACY

V-93411

SWIFT-CSCV1

2.3

VULN-ID

V-205692

Assets

live-malware

NULL

WN19-CC-000340 - Windows Server 2019 must not save passwords 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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205808r1051080_rule
STIG-ID	WN19-CC-000340
STIG-LEGACY	SV-103511
STIG-LEGACY	V-93425
VULN-ID	V-205808

Assets

live-malware

NULL

WN19-CC-000350 - Windows Server 2019 Remote Desktop Services must prevent drive redirection.

Info

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-205722r958524_rule
STIG-ID	WN19-CC-000350
STIG-LEGACY	SV-103619
STIG-LEGACY	V-93533
VULN-ID	V-205722

Assets

live-malware

NULL

WN19-CC-000360 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205809r1051081_rule
STIG-ID	WN19-CC-000360
STIG-LEGACY	SV-103513
STIG-LEGACY	V-93427
VULN-ID	V-205809

Assets

live-malware

NULL

WN19-CC-000370 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (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.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000250-GPOS-00093

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_Server_2019_V3R4_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
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	Windows_Server_2019_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-205636r958408_rule
STIG-ID	WN19-CC-000370
STIG-LEGACY	SV-103059
STIG-LEGACY	V-92971
SWIFT-CSCV1	2.6
VULN-ID	V-205636

Assets

live-malware

NULL

WN19-CC-000380 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High 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.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000250-GPOS-00093

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' with 'High Level' selected.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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
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	Windows_Server_2019_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-205637r958408_rule
STIG-ID	WN19-CC-000380
STIG-LEGACY	SV-103061
STIG-LEGACY	V-92973
SWIFT-CSCV1	2.6
VULN-ID	V-205637

Assets

live-malware

NULL

WN19-CC-000390 - Windows Server 2019 must prevent attachments 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_Server_2019_V3R4_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	Windows_Server_2019_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-205873r991589_rule
STIG-ID	WN19-CC-000390
STIG-LEGACY	SV-103353
STIG-LEGACY	V-93265
SWIFT-CSCV1	2.3
VULN-ID	V-205873

Assets

live-malware

NULL

WN19-CC-000410 - Windows Server 2019 must prevent Indexing of encrypted files.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205694r958478_rule
STIG-ID	WN19-CC-000410
STIG-LEGACY	SV-103501
STIG-LEGACY	V-93415
SWIFT-CSCV1	2.3

VULN-ID

V-205694

Assets

live-malware

NULL

WN19-CC-000420 - Windows Server 2019 must prevent users 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_Server_2019_V3R4_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	Windows_Server_2019_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-205801r1051078_rule
STIG-ID	WN19-CC-000420
STIG-LEGACY	SV-103287
STIG-LEGACY	V-93199
SWIFT-CSCV1	5.1
VULN-ID	V-205801

Assets

live-malware

NULL

WN19-CC-000430 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205802r1051079_rule
STIG-ID	WN19-CC-000430
STIG-LEGACY	SV-103289
STIG-LEGACY	V-93201
SWIFT-CSCV1	5.1
VULN-ID	V-205802

Assets

live-malware

NULL

WN19-CC-000460 - Windows Server 2019 PowerShell script block logging 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.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205639r958422_rule
STIG-ID	WN19-CC-000460
STIG-LEGACY	SV-103263
STIG-LEGACY	V-93175
SWIFT-CSCV1	6.4
VULN-ID	V-205639

Assets

live-malware

NULL

WN19-CC-000470 - Windows Server 2019 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. Disabling Basic authentication will reduce this potential.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205711r958510_rule
STIG-ID	WN19-CC-000470
STIG-LEGACY	SV-103589
STIG-LEGACY	V-93503
TBA-FIISB	45.2.3
VULN-ID	V-205711

Assets

live-malware

NULL

WN19-CC-000480 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	Windows_Server_2019_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-205816r958848_rule
STIG-ID	WN19-CC-000480
STIG-LEGACY	SV-103585
STIG-LEGACY	V-93499
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-205816

Assets

live-malware

NULL

WN19-CC-000490 - Windows Server 2019 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. Disallowing Digest authentication will reduce this potential.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205712r958510_rule
STIG-ID	WN19-CC-000490
STIG-LEGACY	SV-103591
STIG-LEGACY	V-93505
TBA-FIISB	45.2.3
VULN-ID	V-205712

Assets

live-malware

NULL

WN19-CC-000500 - Windows Server 2019 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. Disabling Basic authentication will reduce this potential.

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205713r958510_rule
STIG-ID	WN19-CC-000500
STIG-LEGACY	SV-103593
STIG-LEGACY	V-93507
TBA-FIISB	45.2.3
VULN-ID	V-205713

Assets

live-malware

NULL

WN19-CC-000510 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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
CCI	CCI-003123
CSF	PR.MA-2
DISA_BENCHMARK	Windows_Server_2019_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-205817r958848_rule
STIG-ID	WN19-CC-000510
STIG-LEGACY	SV-103587
STIG-LEGACY	V-93501
SWIFT-CSCV1	2.6
TBA-FIISB	45.2.3
VULN-ID	V-205817

Assets

live-malware

NULL

WN19-CC-000520 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205810r1051082_rule
STIG-ID	WN19-CC-000520
STIG-LEGACY	SV-103515
STIG-LEGACY	V-93429
VULN-ID	V-205810

Assets

live-malware

NULL

WN19-CC-000530 - Windows Server 2019 must have PowerShell Transcription 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.

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_Server_2019_V3R4_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	Windows_Server_2019_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-257503r958420_rule
STIG-ID	WN19-CC-000530
SWIFT-CSCV1	6.4
VULN-ID	V-257503

Assets

live-malware

NULL

WN19-MS-000040 - Windows Server 2019 must restrict unauthenticated Remote Procedure Call (RPC) clients from connecting to the RPC server on domain-joined member servers and standalone or nondomain-joined systems.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205814r971545_rule
STIG-ID	WN19-MS-000040
STIG-LEGACY	SV-103539
STIG-LEGACY	V-93453
TBA-FIISB	27.1
VULN-ID	V-205814

Assets

live-malware

NULL

WN19-MS-000060 - Windows Server 2019 must restrict remote calls to the Security Account Manager (SAM) to Administrators on domain-joined member servers and standalone or nondomain-joined systems.

Info

The Windows SAM stores users' passwords. Restricting Remote Procedure Call (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_Server_2019_V3R4_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	Windows_Server_2019_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-205747r958726_rule
STIG-ID	WN19-MS-000060
STIG-LEGACY	SV-103133
STIG-LEGACY	V-93045
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205747

Assets

live-malware

..

WN19-MS-000070 - Windows Server 2019 'Access this computer from the network' user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems.

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 this right must be limited to those requiring 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 include only the following accounts or groups:

- Administrators
- Authenticated Users

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205671r958472_rule
STIG-ID	WN19-MS-000070
STIG-LEGACY	SV-103095
STIG-LEGACY	V-93007
TBA-FIISB	31.1
VULN-ID	V-205671

Assets

live-malware

'backup operators' && 'users' && 'administrators' && 'everyone'

WN19-MS-000080 - Windows Server 2019 'Deny access to this computer from the network' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from 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' user right defines the accounts that are prevented from logging on from the network.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.

The Guests group must be assigned this right to prevent unauthenticated access.

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 and member of Administrators group' or 'Local account' (see Note below)

All Systems:

- Guests group

Note: These are built-in security groups. 'Local account' is more restrictive but may cause issues on servers such as systems that provide failover clustering.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205672r958472_rule
STIG-ID	WN19-MS-000080
STIG-LEGACY	SV-103097
STIG-LEGACY	V-93009
TBA-FIISB	31.1
VULN-ID	V-205672

Assets

live-malware

NULL

WN19-MS-000090 - Windows Server 2019 'Deny log on as a batch job' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from unauthenticated access on all systems.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The 'Deny log on as a batch job' user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

The Guests group must be assigned to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a batch job' to include the following:

Domain Systems Only:

- Enterprise Admins Group
- Domain Admins Group

All Systems:

- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205673r958472_rule
STIG-ID	WN19-MS-000090
STIG-LEGACY	SV-103099
STIG-LEGACY	V-93011
TBA-FIISB	31.1
VULN-ID	V-205673

Assets

live-malware

NULL

WN19-MS-000110 - Windows Server 2019 'Deny log on locally' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and from 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' user right defines accounts that are prevented from logging on interactively. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. The Guests group must be assigned this right to prevent unauthenticated access.

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

All Systems:

- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205675r958472_rule
STIG-ID	WN19-MS-000110
STIG-LEGACY	SV-103103
STIG-LEGACY	V-93015
TBA-FIISB	31.1
VULN-ID	V-205675

Assets

live-malware

NULL

WN19-MS-000120 - Windows Server 2019 'Deny log on through Remote Desktop Services' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and all local accounts and from 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' user right defines the accounts that are prevented from logging on using Remote Desktop Services.

In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain.

Local accounts on domain-joined systems must also be assigned this right to decrease the risk of lateral movement resulting from credential theft attacks.

The Guests group must be assigned this right to prevent unauthenticated access.

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:

Domain Systems Only:

- Enterprise Admins group
- Domain Admins group
- Local account (see Note below)

All Systems:

- Guests group

Note: 'Local account' is referring to the Windows built-in security group.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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-002314
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	Windows_Server_2019_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-205733r958672_rule
STIG-ID	WN19-MS-000120
STIG-LEGACY	SV-103053
STIG-LEGACY	V-92965
SWIFT-CSCV1	2.6
VULN-ID	V-205733

Assets

live-malware

NULL

WN19-PK-000010 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates 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 CAs. The DoD root certificates will ensure that the trust chain is established for server certificates issued from the DoD CAs.

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

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>. 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_Server_2019_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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)

ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205648r958448_rule
STIG-ID	WN19-PK-000010
STIG-LEGACY	SV-103573
STIG-LEGACY	V-93487
VULN-ID	V-205648

Assets

live-malware

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'
```

WN19-PK-000020 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates 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. Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000403-GPOS-00182

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

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

The FBCA Cross-Certificate Remover Tool and User Guide are available on Cyber Exchange at <https://cyber.mil/pki-pke/tools-configuration-files>.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205649r958448_rule
STIG-ID	WN19-PK-000020
STIG-LEGACY	SV-103575
STIG-LEGACY	V-93489
VULN-ID	V-205649

Assets

live-malware

'No matching certificates found'

WN19-PK-000030 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates 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.

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

Solution

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

Issued To - Issued By - Thumbprint

DoD Root CA 3 - US DoD CCEB Interoperability Root CA 2 - 9B74964506C7ED9138070D08D5F8B969866560C8

DoD Root CA 6 - US DOD CCEB Interoperability Root CA 2 -D471CA32F7A692CE6CBB6196BD3377FE4DBCD106

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

The FBCA Cross-Certificate Remover Tool and User Guide are available on 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_Server_2019_V3R4_STIG.zip

References

800-171	3.5.2
800-171	3.13.15
800-171R3	03.05.12
800-171R3	03.13.15
800-53	IA-5(2)(a)
800-53	SC-23(5)
800-53R5	IA-5(2)(b)(1)
800-53R5	SC-23(5)
CAT	II
CCI	CCI-000185
CCI	CCI-002470
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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)
ITSG-33	SC-23
ITSG-33	SC-23a.
NESA	T4.5.1
NESA	T5.2.3
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205650r1028366_rule
STIG-ID	WN19-PK-000030
STIG-LEGACY	SV-103577
STIG-LEGACY	V-93491
VULN-ID	V-205650

Assets

live-malware

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'
```

WN19-SO-000040 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205910r991589_rule
STIG-ID	WN19-SO-000040
STIG-LEGACY	SV-103371
STIG-LEGACY	V-93283
SWIFT-CSCV1	2.3
VULN-ID	V-205910

Assets

live-malware

' Guest '

WN19-SO-000050 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205644r958442_rule
STIG-ID	WN19-SO-000050
STIG-LEGACY	SV-103239
STIG-LEGACY	V-93151
SWIFT-CSCV1	6.4
VULN-ID	V-205644

Assets

live-malware

NULL

WN19-SO-000120 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.

Info

Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.10
800-171R3	03.01.10
800-171R3	03.01.10a.
800-171R3	03.01.10b.
800-53	AC-11a.
800-53	AC-11b.
800-53	AC-11(1)
800-53R5	AC-11a.
800-53R5	AC-11b.
800-53R5	AC-11(1)
CAT	II
CCI	CCI-000056
CCI	CCI-000057
CCI	CCI-000060
CN-L3	8.1.4.1(b)
DISA_BENCHMARK	Windows_Server_2019_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-11a.
ITSG-33	AC-11b.
ITSG-33	AC-11(1)
NESA	T2.3.8
NESA	T2.3.9
NIAV2	AM23a
NIAV2	AM23b
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM23e
PCI-DSSV3.2.1	8.1.8
PCI-DSSV4.0	8.2.8
RULE-ID	SV-205633r958400_rule
STIG-ID	WN19-SO-000120
STIG-LEGACY	SV-103049
STIG-LEGACY	V-92961
VULN-ID	V-205633

Assets

live-malware

NULL

WN19-SO-000130 - Windows Server 2019 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-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.9
800-171R3	03.01.09
800-53	AC-8a.
800-53	AC-8b.
800-53	AC-8c.1.
800-53	AC-8c.2.
800-53	AC-8c.3.
800-53R5	AC-8a.
800-53R5	AC-8b.
800-53R5	AC-8c.1.
800-53R5	AC-8c.2.
800-53R5	AC-8c.3.
CAT	II
CCI	CCI-000048
CCI	CCI-000050
CCI	CCI-001384
CCI	CCI-001385

CCI	CCI-001386
CCI	CCI-001387
CCI	CCI-001388
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.5
ITSG-33	AC-8a.
ITSG-33	AC-8b.
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
NIAV2	AM10f
RULE-ID	SV-205631r958390_rule
STIG-ID	WN19-SO-000130
STIG-LEGACY	SV-103235
STIG-LEGACY	V-93147
TBA-FIISB	45.2.4
VULN-ID	V-205631

Assets

live-malware

'No content provided to compare with.'

WN19-SO-000140 - Windows Server 2019 title for legal banner dialog box must be configured with the appropriate text.

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-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

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 an organization-defined equivalent.

If an organization-defined title is used, it can in no case contravene or modify the language of the message text required in WN19-SO-000130.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205632r958390_rule
STIG-ID	WN19-SO-000140
STIG-LEGACY	SV-103237
STIG-LEGACY	V-93149
TBA-FIISB	45.2.4
VULN-ID	V-205632

Assets

live-malware

'No content provided to compare with.'

WN19-SO-000150 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205912r991589_rule
STIG-ID	WN19-SO-000150
STIG-LEGACY	SV-103375
STIG-LEGACY	V-93287
SWIFT-CSCV1	2.3
VULN-ID	V-205912

Assets

live-malware

'0'

WN19-SO-000160 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.

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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205825r958908_rule

STIG-ID	WN19-SO-000160
STIG-LEGACY	SV-103641
STIG-LEGACY	V-93555
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205825

Assets

live-malware

0

WN19-SO-000190 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.

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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205827r958908_rule

STIG-ID	WN19-SO-000190
STIG-LEGACY	SV-103645
STIG-LEGACY	V-93559
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205827

Assets

live-malware

0

WN19-SO-000200 - Windows Server 2019 setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.

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 negotiate SMB packet signing as requested by the client.

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

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205828r958908_rule

STIG-ID	WN19-SO-000200
STIG-LEGACY	SV-103647
STIG-LEGACY	V-93561
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205828

Assets

live-malware

0

WN19-SO-000230 - Windows Server 2019 must not allow anonymous enumeration of shares.

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-205724r958524_rule
STIG-ID	WN19-SO-000230
STIG-LEGACY	SV-103623
STIG-LEGACY	V-93537
VULN-ID	V-205724

Assets

live-malware

0

WN19-SO-000260 - Windows Server 2019 services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.

Info

Services using Local System that use Negotiate when reverting to NTLM authentication may gain unauthorized access if allowed to authenticate anonymously versus using the computer identity.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205916r991589_rule
STIG-ID	WN19-SO-000260
STIG-LEGACY	SV-103383
STIG-LEGACY	V-93295
SWIFT-CSCV1	2.3
VULN-ID	V-205916

Assets

live-malware

NULL

WN19-SO-000270 - Windows Server 2019 must prevent NTLM 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_Server_2019_V3R4_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	Windows_Server_2019_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-205917r991589_rule
STIG-ID	WN19-SO-000270
STIG-LEGACY	SV-103385
STIG-LEGACY	V-93297
SWIFT-CSCV1	2.3
VULN-ID	V-205917

Assets

live-malware

NULL

WN19-SO-000280 - Windows Server 2019 must prevent PKU2U authentication using online identities.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205918r991589_rule
STIG-ID	WN19-SO-000280
STIG-LEGACY	SV-103387
STIG-LEGACY	V-93299
SWIFT-CSCV1	2.3
VULN-ID	V-205918

Assets

live-malware

NULL

WN19-SO-000290 - Windows Server 2019 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. The DES and RC4 encryption suites must not be used for Kerberos encryption.

Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting 'The other domain supports Kerberos AES Encryption' on domain trusts, may be required to allow client communication across the trust relationship.

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

Note: Organizations with domain controllers running earlier versions of Windows where RC4 encryption is enabled, selecting 'The other domain supports Kerberos AES Encryption' on domain trusts, may be required to allow client communication across the trust relationship.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205708r971535_rule
STIG-ID	WN19-SO-000290
STIG-LEGACY	SV-103581

STIG-LEGACY

V-93495

VULN-ID

V-205708

Assets

live-malware

NULL

WN19-SO-000310 - Windows Server 2019 LAN Manager authentication level must be configured 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 standalone or nondomain-joined 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_Server_2019_V3R4_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	Windows_Server_2019_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-205919r991589_rule
STIG-ID	WN19-SO-000310
STIG-LEGACY	SV-103389
STIG-LEGACY	V-93301
SWIFT-CSCV1	2.3
VULN-ID	V-205919

Assets

live-malware

NULL

WN19-SO-000330 - Windows Server 2019 session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.

Info

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205921r991589_rule
STIG-ID	WN19-SO-000330
STIG-LEGACY	SV-103393
STIG-LEGACY	V-93305
SWIFT-CSCV1	2.3
VULN-ID	V-205921

Assets

live-malware

536870912

WN19-SO-000340 - Windows Server 2019 session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.

Info

Microsoft has implemented a variety of security support providers for use with Remote Procedure Call (RPC) sessions. All of the options must be enabled to ensure the maximum security level.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205922r991589_rule
STIG-ID	WN19-SO-000340
STIG-LEGACY	SV-103395
STIG-LEGACY	V-93307
SWIFT-CSCV1	2.3
VULN-ID	V-205922

Assets

live-malware

536870912

WN19-SO-000350 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer.

Info

If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'System cryptography: Force strong key protection for user keys stored on the computer' to 'User must enter a password each time they use a key'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.2
800-171R3	03.05.12
800-53	IA-5(2)(b)
800-53R5	IA-5(2)(a)(1)
CAT	II
CCI	CCI-000186
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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)(b)
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205651r958450_rule

STIG-ID	WN19-SO-000350
---------	----------------

STIG-LEGACY	SV-103579
-------------	-----------

STIG-LEGACY	V-93493
-------------	---------

VULN-ID	V-205651
---------	----------

Assets

live-malware

NULL

WN19-SO-000360 - Windows Server 2019 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.

Info

This setting ensures the system uses algorithms that are FIPS-compliant for encryption, hashing, and signing. FIPS-compliant algorithms meet specific standards established by the U.S. Government and must be the algorithms used for all OS encryption functions.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205842r1028367_rule
STIG-ID	WN19-SO-000360
STIG-LEGACY	SV-103597
STIG-LEGACY	V-93511
VULN-ID	V-205842

Assets

live-malware

0

WN19-SO-000380 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205811r1051083_rule
STIG-ID	WN19-SO-000380
STIG-LEGACY	SV-103517
STIG-LEGACY	V-93431
VULN-ID	V-205811

Assets

live-malware

NULL

WN19-SO-000400 - Windows Server 2019 User Account Control must, at a minimum, 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'.

The more secure option for this setting, 'Prompt for credentials on the secure desktop', would also be acceptable.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205717r958518_rule
STIG-ID	WN19-SO-000400
STIG-LEGACY	SV-103609
STIG-LEGACY	V-93523
VULN-ID	V-205717

Assets

live-malware

WN19-SO-000410 - Windows Server 2019 User Account Control must automatically deny standard user requests for elevation.

Info

User Account Control (UAC) is a security mechanism for limiting the elevation of privileges, including administrative accounts, unless authorized. This setting controls the behavior of elevation when requested by a standard user account.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205812r1051084_rule
STIG-ID	WN19-SO-000410
STIG-LEGACY	SV-103519
STIG-LEGACY	V-93433
VULN-ID	V-205812

Assets

live-malware

WN19-UR-000030 - Windows Server 2019 Allow log on locally 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 '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 include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205676r958472_rule
STIG-ID	WN19-UR-000030
STIG-LEGACY	SV-103105
STIG-LEGACY	V-93017
TBA-FIISB	31.1
VULN-ID	V-205676

Assets

live-malware

```
'backup operators' && 'users' && 'administrators'
```

WN19-UR-000040 - Windows Server 2019 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 include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205751r958726_rule
STIG-ID	WN19-UR-000040
STIG-LEGACY	SV-103141
STIG-LEGACY	V-93053
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205751

Assets

live-malware

'backup operators' && 'administrators'

WN19-UR-000140 - Windows Server 2019 Increase scheduling priority: 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 'Increase scheduling priority' user right can change a scheduling priority, causing performance issues or a denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Increase scheduling priority' to include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205761r958726_rule
STIG-ID	WN19-UR-000140
STIG-LEGACY	SV-103161
STIG-LEGACY	V-93073
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205761

Assets

live-malware

```
'window manager group' && 'administrators'
```

WN19-UR-000210 - Windows Server 2019 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 overwrite 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 include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205767r958726_rule
STIG-ID	WN19-UR-000210
STIG-LEGACY	SV-103173
STIG-LEGACY	V-93085
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205767

Assets

live-malware

'backup operators' && 'administrators'

Audits SKIPPED

Audits PASSED

DISA_Microsoft_Windows_Server_2019_STIG_v3r4.audit from DISA Microsoft Windows Server 2019 STIG v3r4

Info

Solution

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

Assets

live-malware

All of the following must pass to satisfy this requirement:

PASSED - Windows Server 2019 is installed:

Remote value: 'Windows Server 2019 Datacenter'

Policy value: '^ [a-zA-Z0-9\\(\\)\\s]*2019[\\s]*[a-zA-Z0-9\\(\\)\\s:]*\$'

WN19-00-000040 - Windows Server 2019 members of the Backup Operators group must have separate accounts for backup duties and normal operational tasks.

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

Ensure each member of the Backup Operators group has separate accounts for backup functions and standard user functions.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205846r991589_rule
STIG-ID	WN19-00-000040
STIG-LEGACY	SV-103295
STIG-LEGACY	V-93207
SWIFT-CSCV1	2.3
VULN-ID	V-205846

Assets

live-malware

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.'

WN19-00-000060 - Windows Server 2019 manually managed application account passwords must be changed at least annually or when a system administrator with knowledge of the password leaves the organization.

Info

Setting application account passwords to expire may cause applications to stop functioning. However, not changing them on a regular basis exposes them to attack. If managed service accounts are used, this alleviates the need to manually change application account passwords.

Solution

Change passwords for manually managed application/service accounts at least annually or when an administrator with knowledge of the password leaves the organization.

It is recommended that system-managed service accounts be used whenever possible.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205847r991589_rule
STIG-ID	WN19-00-000060
STIG-LEGACY	SV-103297
STIG-LEGACY	V-93209
SWIFT-CSCV1	2.3
VULN-ID	V-205847

Assets

live-malware

'No service account with password older than 365 days'

WN19-00-000090 - Windows Server 2019 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.

Info

Credential Guard uses virtualization-based security to protect data that could be used in credential theft attacks if compromised. A number of system requirements 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

Ensure domain-joined systems have a TPM that is configured for use. (Versions 2.0 or 1.2 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_Server_2019_V3R4_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	Windows_Server_2019_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-205848r991589_rule
STIG-ID	WN19-00-000090
STIG-LEGACY	SV-103301
STIG-LEGACY	V-93213
SWIFT-CSCV1	2.3
VULN-ID	V-205848

Assets

live-malware

PASSED

WN19-00-000100 - Windows Server 2019 must be maintained at a supported servicing level.

Info

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

Solution

Update the system to a Version 1809 (Build 17763.xxx) or greater.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205849r991589_rule
STIG-ID	WN19-00-000100
STIG-LEGACY	SV-103303
STIG-LEGACY	V-93215
SWIFT-CSCV1	2.3
VULN-ID	V-205849

Assets

live-malware

'17763'

WN19-00-000130 - Windows Server 2019 local volumes must use a format that supports NTFS attributes.

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 a file system that supports NTFS attributes.

Solution

Format volumes to use NTFS or ReFS.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205663r958472_rule
STIG-ID	WN19-00-000130
STIG-LEGACY	SV-103079
STIG-LEGACY	V-92991
TBA-FIISB	31.1
VULN-ID	V-205663

Assets

live-malware

'None '

WN19-00-000150 - Windows Server 2019 permissions for program file 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.

The default permissions are adequate when the Security Option 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (WN19-SO-000240).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Solution

Maintain the default permissions for the program file directories and configure the Security Option 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (WN19-SO-000240).

Default permissions:

\Program Files and \Program Files (x86) Type - 'Allow' for all Inherited from - 'None' for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders SYSTEM - Modify - This folder only SYSTEM - Full control -

Subfolders and files only Administrators - Modify - This folder only Administrators - Full control - Subfolders and files

only Users - Read & execute - This folder, subfolders, and files CREATOR OWNER - Full control - Subfolders and

files only ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files ALL RESTRICTED

APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205735r958702_rule
STIG-ID	WN19-00-000150
STIG-LEGACY	SV-103109
STIG-LEGACY	V-93021
TBA-FIISB	31.1
VULN-ID	V-205735

Assets

live-malware

All of the following must pass to satisfy this requirement:

```
-----
PASSED - c:\program files:
  Remote value: 'C:\Program Files NT SERVICE\TrustedInstaller:(F)
                NT SERVICE\TrustedInstaller:(CI)(IO)(F)
                NT AUTHORITY\SYSTEM:(M)
                NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
```

```
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)
(GR,GE)
```

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
Policy value: 'STATUS: PASSED'

PASSED - Program Files (x86) permissions:

```
Remote value: 'C:\Program Files (x86) NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION [...]
```


WN19-00-000160 - Windows Server 2019 permissions for the Windows installation directory 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.

The default permissions are adequate when the Security Option 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (WN19-SO-000240).

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124

Solution

Maintain the default file ACLs and configure the Security Option 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled' (WN19-SO-000240).

Default permissions:

Type - 'Allow' for all Inherited from - 'None' for all

Principal - Access - Applies to

TrustedInstaller - Full control - This folder and subfolders SYSTEM - Modify - This folder only SYSTEM - Full control -

Subfolders and files only Administrators - Modify - This folder only Administrators - Full control - Subfolders and files

only Users - Read & execute - This folder, subfolders, and files CREATOR OWNER - Full control - Subfolders and

files only ALL APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files ALL RESTRICTED

APPLICATION PACKAGES - Read & execute - This folder, subfolders, and files

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205736r1016383_rule
STIG-ID	WN19-00-000160
STIG-LEGACY	SV-103111
STIG-LEGACY	V-93023
TBA-FIISB	31.1
VULN-ID	V-205736

Assets

live-malware

```
'C:\Windows NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
```

CREATOR OWNER:(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'

WN19-00-000170 - Windows Server 2019 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 - Subkeys only ALL APPLICATION PACKAGES - Read - This key and subkeys Server Operators - Read - This Key and subkeys (Domain controllers only)

Microsoft has also given Read permission to the SOFTWARE and SYSTEM registry keys in Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205737r958726_rule
STIG-ID	WN19-00-000170
STIG-LEGACY	SV-103113
STIG-LEGACY	V-93025
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205737

Assets

live-malware

All of the following must pass to satisfy this requirement:

```
-----
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 dac' | 'write owner'

all application packages:
+ Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'enumerate subkeys' | 'notify' | 'query value' | 'read control'

creator owner:
+ 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'

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'

users:
+ Apply To: 'this key and subkeys'
  |- Inheritance: 'not inherited'
  |- Allow: 'enumerate subkeys' | [...]

```

WN19-00-000200 - Windows Server 2019 accounts must require passwords.

Info

The lack of password protection enables anyone to gain access to the information system, which opens a backdoor opportunity for intruders to compromise the system as well as other resources. Accounts on a system must require passwords.

Solution

Configure all enabled accounts to require passwords.

The password required flag can be set by entering the following on a command line: 'Net user [username] / passwordreq:yes', substituting [username] with the name of the user account.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205700r958482_rule
STIG-ID	WN19-00-000200
STIG-LEGACY	SV-103525
STIG-LEGACY	V-93439
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205700

Assets

live-malware

'All users require passwords'

WN19-00-000210 - Windows Server 2019 passwords must be configured to expire.

Info

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

Solution

Configure all enabled user account passwords to expire.

Uncheck 'Password never expires' for all enabled user accounts in Active Directory Users and Computers for domain accounts and Users in Computer Management for member servers and standalone or nondomain-joined systems.

Document any exceptions with the ISSO.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205658r1051066_rule
STIG-ID	WN19-00-000210
STIG-LEGACY	SV-103561
STIG-LEGACY	V-93475
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-205658

Assets

live-malware

'All users passwords expire'

WN19-00-000230 - Windows Server 2019 non-system-created file shares must limit access to groups that require it.

Info

Shares on a system provide network access. To prevent exposing sensitive information, where shares are necessary, permissions must be reconfigured to give the minimum access to accounts that require it.

NOTE: Nessus has provided the target output to assist in reviewing 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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-205721r958524_rule
STIG-ID	WN19-00-000230
STIG-LEGACY	SV-103617
STIG-LEGACY	V-93531
VULN-ID	V-205721

Assets

live-malware

WN19-00-000320 - Windows Server 2019 must not have the Fax Server role installed.

Info

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

Solution

Uninstall the 'Fax Server' role.
Start 'Server Manager'.
Select the server with the role.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'Fax Server' on the 'Roles' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205678r958478_rule

STIG-ID	WN19-00-000320
STIG-LEGACY	SV-103469
STIG-LEGACY	V-93383
SWIFT-CSCV1	2.3
VULN-ID	V-205678

Assets

live-malware

'HKLM\System\CurrentControlSet\Services\Fax_registry_does_not_exist'

WN19-00-000330 - Windows Server 2019 must not have the Microsoft FTP service installed unless required by the organization.

Info

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

Solution

Uninstall the 'FTP Server' role.
Start 'Server Manager'.
Select the server with the role.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'FTP Server' under 'Web Server (IIS)' on the 'Roles' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205697r958480_rule
STIG-ID	WN19-00-000330
STIG-LEGACY	SV-103507
STIG-LEGACY	V-93421
SWIFT-CSCV1	2.3
VULN-ID	V-205697

Assets

live-malware

'HKLM\System\CurrentControlSet\Services\FTPSVC_registry_does_not_exist'

WN19-00-000340 - Windows Server 2019 must not have the Peer Name Resolution Protocol installed.

Info

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

Solution

Uninstall the 'Peer Name Resolution Protocol' feature.
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'Peer Name Resolution Protocol' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205679r958478_rule

STIG-ID	WN19-00-000340
STIG-LEGACY	SV-103471
STIG-LEGACY	V-93385
SWIFT-CSCV1	2.3
VULN-ID	V-205679

Assets

live-malware

'HKLM\System\CurrentControlSet\Services\PNRPsvc_registry_does_not_exist'

WN19-00-000350 - Windows Server 2019 must not have Simple TCP/IP Services installed.

Info

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

Solution

Uninstall the 'Simple TCP/IP Services' feature.
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'Simple TCP/IP Services' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205680r958478_rule

STIG-ID	WN19-00-000350
STIG-LEGACY	SV-103473
STIG-LEGACY	V-93387
SWIFT-CSCV1	2.3
VULN-ID	V-205680

Assets

live-malware

'HKLM\System\CurrentControlSet\Services\simptcp_registry_does_not_exist'

WN19-00-000360 - Windows Server 2019 must not have the Telnet Client installed.

Info

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

Solution

Uninstall the 'Telnet Client' feature.
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'Telnet Client' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205698r958480_rule
STIG-ID	WN19-00-000360
STIG-LEGACY	SV-103509
STIG-LEGACY	V-93423
SWIFT-CSCV1	2.3
VULN-ID	V-205698

Assets

live-malware

'InstallState : Available'

WN19-00-000370 - Windows Server 2019 must not have the TFTP Client installed.

Info

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

Solution

Uninstall the 'TFTP Client' feature.
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'TFTP Client' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205681r958478_rule

STIG-ID	WN19-00-000370
STIG-LEGACY	SV-103475
STIG-LEGACY	V-93389
SWIFT-CSCV1	2.3
VULN-ID	V-205681

Assets

live-malware

'InstallState : Available'

WN19-00-000380 - Windows Server 2019 must not have the Server Message Block (SMB) v1 protocol installed.

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 and is not FIPS compliant.

Solution

Uninstall the SMBv1 protocol.
Open 'Windows PowerShell' with elevated privileges (run as administrator).
Enter 'Uninstall-WindowsFeature -Name FS-SMB1 -Restart'.
(Omit the Restart parameter if an immediate restart of the system cannot be done.)
Alternately:
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'SMB 1.0/CIFS File Sharing Support' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205682r958478_rule
STIG-ID	WN19-00-000380
STIG-LEGACY	SV-103477
STIG-LEGACY	V-93391
SWIFT-CSCV1	2.3
VULN-ID	V-205682

Assets

live-malware

'InstallState : Removed'

WN19-00-000410 - Windows Server 2019 must not have Windows PowerShell 2.0 installed.

Info

Windows PowerShell 5.x added advanced logging features that can provide additional detail when malware has been run on a system. Disabling the Windows PowerShell 2.0 mitigates against a downgrade attack that evades the Windows PowerShell 5.x script block logging feature.

Solution

Uninstall the 'Windows PowerShell 2.0 Engine'.
Start 'Server Manager'.
Select the server with the feature.
Scroll down to 'ROLES AND FEATURES' in the right pane.
Select 'Remove Roles and Features' from the drop-down 'TASKS' list.
Select the appropriate server on the 'Server Selection' page and click 'Next'.
Deselect 'Windows PowerShell 2.0 Engine' under 'Windows PowerShell' on the 'Features' page.
Click 'Next' and 'Remove' as prompted.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205685r958478_rule

STIG-ID	WN19-00-000410
STIG-LEGACY	SV-103483
STIG-LEGACY	V-93397
SWIFT-CSCV1	2.3
VULN-ID	V-205685

Assets

live-malware

'InstallState : Removed'

WN19-00-000440 - The Windows Server 2019 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, which are identified at:

<https://www.cnmc.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_Server_2019_V3R4_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	Windows_Server_2019_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-205800r1051077_rule
STIG-ID	WN19-00-000440
STIG-LEGACY	SV-103275
STIG-LEGACY	V-93187
TBA-FIISB	37.4
VULN-ID	V-205800

Assets

live-malware

```
'NtpServer: time.windows.com,0x8 (Local)
NtpServer (Local)'
```

WN19-00-000460 - Windows Server 2019 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, 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_Server_2019_V3R4_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	Windows_Server_2019_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-205856r991589_rule
STIG-ID	WN19-00-000460
STIG-LEGACY	SV-103317
STIG-LEGACY	V-93229
SWIFT-CSCV1	2.3
VULN-ID	V-205856

Assets

live-malware

'path' \Windows\system32\winload.efi'

WN19-00-000470 - Windows Server 2019 must have Secure Boot enabled.

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, 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_Server_2019_V3R4_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	Windows_Server_2019_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-205857r991589_rule
STIG-ID	WN19-00-000470
STIG-LEGACY	SV-103319
STIG-LEGACY	V-93231
SWIFT-CSCV1	2.3
VULN-ID	V-205857

Assets

live-malware

'True'

WN19-AC-000050 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205659r1051067_rule
STIG-ID	WN19-AC-000050
STIG-LEGACY	SV-103563
STIG-LEGACY	V-93477
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.2
VULN-ID	V-205659

Assets

live-malware

42

WN19-AC-000080 - Windows Server 2019 must have the built-in Windows password complexity policy enabled.

Info

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

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

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_Server_2019_V3R4_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-000193
CCI	CCI-000194
CCI	CCI-001619
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	Windows_Server_2019_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-205652r1051061_rule
STIG-ID	WN19-AC-000080
STIG-LEGACY	SV-103545
STIG-LEGACY	V-93459
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-205652

Assets

live-malware

'enabled'

WN19-AC-000090 - Windows Server 2019 reversible password encryption must be disabled.

Info

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205653r1051062_rule
STIG-ID	WN19-AC-000090

STIG-LEGACY	SV-103551
STIG-LEGACY	V-93465
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-205653

Assets

live-malware

'disabled'

WN19-AU-000030 - Windows Server 2019 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.

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

Solution

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

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

The default location is the '%SystemRoot%\System32\winevt\Logs' folder.

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_Server_2019_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	Windows_Server_2019_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-205640r958434_rule
STIG-ID	WN19-AU-000030
STIG-LEGACY	SV-103277
STIG-LEGACY	V-93189
VULN-ID	V-205640

Assets

live-malware

```
'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'
```

WN19-AU-000040 - Windows Server 2019 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.

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

Solution

Configure the permissions on the Security event log file (Security.evtx) to prevent access by non-privileged accounts.

The default permissions listed below satisfy this requirement:

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

The default location is the '%SystemRoot%\System32\winevt\Logs' folder.

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_Server_2019_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	Windows_Server_2019_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-205641r958434_rule
STIG-ID	WN19-AU-000040
STIG-LEGACY	SV-103279
STIG-LEGACY	V-93191
VULN-ID	V-205641

Assets

live-malware

```
'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'

WN19-AU-000050 - Windows Server 2019 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.

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

Solution

Configure the permissions on the System event log file (System.evtx) to prevent access by non-privileged accounts.

The default permissions listed below satisfy this requirement:

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

The default location is the '%SystemRoot%\System32\winevt\Logs' folder.

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_Server_2019_V3R4_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
CCI	CCI-000163
CCI	CCI-000164
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	Windows_Server_2019_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-205642r958434_rule
STIG-ID	WN19-AU-000050
STIG-LEGACY	SV-103281
STIG-LEGACY	V-93193
VULN-ID	V-205642

Assets

live-malware

```
'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'
```

WN19-AU-000060 - Windows Server 2019 Event Viewer must be protected from unauthorized modification and deletion.

Info

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information. Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the modification or deletion of audit tools.
Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Solution

Configure the permissions on the 'Eventvwr.exe' file to prevent modification by any groups or accounts other than TrustedInstaller. The default permissions listed below satisfy this requirement:
TrustedInstaller - Full Control Administrators, SYSTEM, Users, ALL APPLICATION PACKAGES, ALL RESTRICTED APPLICATION PACKAGES - Read & Execute
The default location is the '%SystemRoot%\System32' folder.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.3.8
800-171R3	03.03.08
800-53	AU-9
800-53R5	AU-9
CAT	II
CCI	CCI-001494
CCI	CCI-001495
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	Windows_Server_2019_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-205731r991558_rule
STIG-ID	WN19-AU-000060
STIG-LEGACY	SV-103283
STIG-LEGACY	V-93195
VULN-ID	V-205731

Assets

live-malware

```
'C:\Windows\System32\Eventvwr.exe NT SERVICE\TrustedInstaller:(F)
      BUILTIN\Administrators:(RX)
      NT AUTHORITY\SYSTEM:(RX)
      BUILTIN\Users:(RX)
      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION
PACKAGES:(RX)

Successfully processed 1 files; Failed processing 0 files

STATUS: PASSED'
```

WN19-AU-000070 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205832r991578_rule
STIG-ID	WN19-AU-000070
STIG-LEGACY	SV-103241
STIG-LEGACY	V-93153
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205832

Assets

live-malware

'success'

WN19-AU-000090 - Windows Server 2019 must be configured to audit Account Management - Other Account Management 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.

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)

CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4

NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205769r958732_rule
STIG-ID	WN19-AU-000090
STIG-LEGACY	SV-103177
STIG-LEGACY	V-93089
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205769

Assets

live-malware

'success, failure'

WN19-AU-000100 - Windows Server 2019 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 security groups, including changes in group members.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CN-L3	7.1.3.2(d)
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.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-2(4)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5

NESA	T3.6.6
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205625r958368_rule
STIG-ID	WN19-AU-000100
STIG-LEGACY	SV-103067
STIG-LEGACY	V-92979
SWIFT-CSCV1	6.4
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-205625

Assets

live-malware

'success, failure'

WN19-AU-000110 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CN-L3	7.1.3.2(d)
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.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-2(4)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5

NESA	T3.6.6
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205626r958368_rule
STIG-ID	WN19-AU-000110
STIG-LEGACY	SV-103069
STIG-LEGACY	V-92981
SWIFT-CSCV1	6.4
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-205626

Assets

live-malware

'success, failure'

WN19-AU-000120 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CN-L3	7.1.3.2(d)
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.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-2(4)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5

NESA	T3.6.6
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205627r958368_rule
STIG-ID	WN19-AU-000120
STIG-LEGACY	SV-103071
STIG-LEGACY	V-92983
SWIFT-CSCV1	6.4
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-205627

Assets

live-malware

'success, failure'

WN19-AU-000130 - Windows Server 2019 must be configured to audit Detailed Tracking - Plug and Play 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.

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

Solution

Configure the policy value for 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_Server_2019_V3R4_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	Windows_Server_2019_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-205839r991583_rule
STIG-ID	WN19-AU-000130
STIG-LEGACY	SV-103245
STIG-LEGACY	V-93157
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205839

Assets

live-malware

'success, failure'

WN19-AU-000160 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-001404
CN-L3	7.1.3.2(d)
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.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-2(4)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d

NIAV2	AM9e
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205730r991552_rule
STIG-ID	WN19-AU-000160
STIG-LEGACY	SV-103077
STIG-LEGACY	V-92989
SWIFT-CSCV1	6.4
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-205730

Assets

live-malware

'success, failure'

WN19-AU-000180 - Windows Server 2019 must be configured to audit 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.

Satisfies: SRG-OS-000472-GPOS-00217, SRG-OS-000480-GPOS-00227

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_Server_2019_V3R4_STIG.zip

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.2
800-171R3	03.03.03a.
800-171R3	03.04.02a.
800-53	AU-12c.
800-53	CM-6b.
800-53R5	AU-12c.
800-53R5	CM-6b.
CAT	II
CCI	CCI-000172
CCI	CCI-000366
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)
CN-L3	8.1.10.6(d)
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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.12.4.1
ITSG-33	AU-12c.
ITSG-33	CM-6b.
NESA	T3.2.1
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-205838r991581_rule
STIG-ID	WN19-AU-000180
STIG-LEGACY	SV-103259
STIG-LEGACY	V-93171
SWIFT-CSCV1	2.3

SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205838

Assets

live-malware

'success'

WN19-AU-000190 - Windows Server 2019 must be configured to audit 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.12
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.12
800-171R3	03.03.03a.
800-53	AC-17(1)
800-53	AU-12c.
800-53R5	AC-17(1)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000067
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)
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-3
CSF	PR.PT-1
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-17(1)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.4.4
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-205634r958406_rule
STIG-ID	WN19-AU-000190
STIG-LEGACY	SV-103055
STIG-LEGACY	V-92967
SWIFT-CSCV1	2.6
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205634

Assets

live-malware

'success, failure'

WN19-AU-000200 - Windows Server 2019 must be configured to audit 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.12
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.12
800-171R3	03.03.03a.
800-53	AC-17(1)
800-53	AU-12c.
800-53R5	AC-17(1)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000067
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)
CN-L3	8.1.4.4(c)
CN-L3	8.1.10.6(i)
CSF	DE.CM-1

CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-3
CSF	PR.PT-1
CSF	PR.PT-4
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.16
ISO/IEC-27001	A.6.2.2
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-17(1)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.4.4
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
QCSC-V1	13.2
RULE-ID	SV-205635r958406_rule
STIG-ID	WN19-AU-000200
STIG-LEGACY	SV-103057
STIG-LEGACY	V-92969
SWIFT-CSCV1	2.6
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205635

Assets

live-malware

'success, failure'

WN19-AU-000210 - Windows Server 2019 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 that have administrative privileges and can be used to elevate processes.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205835r991578_rule
STIG-ID	WN19-AU-000210
STIG-LEGACY	SV-103249
STIG-LEGACY	V-93161
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205835

Assets

live-malware

'success'

WN19-AU-000220 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205836r991578_rule
STIG-ID	WN19-AU-000220
STIG-LEGACY	SV-103251
STIG-LEGACY	V-93163
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205836

Assets

live-malware

'success, failure'

WN19-AU-000230 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205837r991578_rule
STIG-ID	WN19-AU-000230
STIG-LEGACY	SV-103253
STIG-LEGACY	V-93165
SWIFT-CSCV1	6.4
TBA-FIISB	45.1.1
VULN-ID	V-205837

Assets

live-malware

'success, failure'

WN19-AU-000260 - Windows Server 2019 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.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205771r958732_rule
STIG-ID	WN19-AU-000260
STIG-LEGACY	SV-103181
STIG-LEGACY	V-93093
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205771

Assets

live-malware

'success, failure'

WN19-AU-000270 - Windows Server 2019 must be configured to audit Policy Change - Audit 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 Policy Change records events related to changes in audit policy.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205772r958732_rule
STIG-ID	WN19-AU-000270
STIG-LEGACY	SV-103183
STIG-LEGACY	V-93095
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205772

Assets

live-malware

'success, failure'

WN19-AU-000280 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)

CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4

NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205773r958732_rule
STIG-ID	WN19-AU-000280
STIG-LEGACY	SV-103185
STIG-LEGACY	V-93097
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205773

Assets

live-malware

'success'

WN19-AU-000340 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205779r958732_rule
STIG-ID	WN19-AU-000340
STIG-LEGACY	SV-103197
STIG-LEGACY	V-93109
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205779

Assets

live-malware

'success, failure'

WN19-AU-000350 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205780r958732_rule
STIG-ID	WN19-AU-000350
STIG-LEGACY	SV-103199
STIG-LEGACY	V-93111
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205780

Assets

live-malware

'success, failure'

WN19-AU-000360 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205781r958732_rule
STIG-ID	WN19-AU-000360
STIG-LEGACY	SV-103201
STIG-LEGACY	V-93113
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205781

Assets

live-malware

'success'

WN19-AU-000370 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205782r958732_rule
STIG-ID	WN19-AU-000370
STIG-LEGACY	SV-103203
STIG-LEGACY	V-93115
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205782

Assets

live-malware

'success, failure'

WN19-AU-000380 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205783r958732_rule
STIG-ID	WN19-AU-000380
STIG-LEGACY	SV-103205
STIG-LEGACY	V-93117
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205783

Assets

live-malware

'success, failure'

WN19-AU-000390 - Windows Server 2019 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.

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

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_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205784r958732_rule
STIG-ID	WN19-AU-000390
STIG-LEGACY	SV-103207
STIG-LEGACY	V-93119
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205784

Assets

live-malware

'success, failure'

WN19-CC-000110 - Windows Server 2019 virtualization-based security must be enabled 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

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. A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link:

<https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard>

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205864r991589_rule
STIG-ID	WN19-CC-000110
STIG-LEGACY	SV-103333
STIG-LEGACY	V-93245
SWIFT-CSCV1	2.3

VULN-ID

V-205864

Assets

live-malware

PASSED

WN19-CC-000130 - Windows Server 2019 Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.

Info

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

Solution

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

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205865r991589_rule
STIG-ID	WN19-CC-000130
STIG-LEGACY	SV-103337
STIG-LEGACY	V-93249
SWIFT-CSCV1	2.3
VULN-ID	V-205865

Assets

live-malware

NULL

WN19-CC-000310 - Windows Server 2019 Explorer Data Execution Prevention must be enabled.

Info

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

Solution

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

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-53	SI-16
800-53R5	SI-16
CAT	II
CCI	CCI-002824
CSF2.0	PR.DS-10
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
RULE-ID	SV-205830r958928_rule
STIG-ID	WN19-CC-000310
STIG-LEGACY	SV-103649
STIG-LEGACY	V-93563
VULN-ID	V-205830

Assets

live-malware

NULL

WN19-CC-000320 - Windows Server 2019 Turning off 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 disabled.

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205871r991589_rule
STIG-ID	WN19-CC-000320
STIG-LEGACY	SV-103349
STIG-LEGACY	V-93261
SWIFT-CSCV1	2.3
VULN-ID	V-205871

Assets

live-malware

NULL

WN19-CC-000330 - Windows Server 2019 File Explorer shell protocol must run in protected mode.

Info

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

Solution

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

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205872r991589_rule
STIG-ID	WN19-CC-000330
STIG-LEGACY	SV-103351
STIG-LEGACY	V-93263
SWIFT-CSCV1	2.3
VULN-ID	V-205872

Assets

live-malware

NULL

WN19-CC-000400 - Windows Server 2019 must disable Basic authentication for RSS feeds over HTTP.

Info

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

Solution

The default behavior is for the Windows RSS platform to not use Basic authentication over HTTP connections. If this needs to be corrected, configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> RSS Feeds >> 'Turn on Basic feed authentication over HTTP' to 'Not Configured' or 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205693r958478_rule
STIG-ID	WN19-CC-000400
STIG-LEGACY	SV-103499

STIG-LEGACY V-93413

SWIFT-CSCV1 2.3

VULN-ID V-205693

Assets

live-malware

NULL

WN19-CC-000440 - Windows Server 2019 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.

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205874r991589_rule
STIG-ID	WN19-CC-000440
STIG-LEGACY	SV-103355
STIG-LEGACY	V-93267
SWIFT-CSCV1	2.3
VULN-ID	V-205874

Assets

live-malware

NULL

WN19-CC-000450 - Windows Server 2019 must disable automatically signing in the last interactive user after a system-initiated restart.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205925r991591_rule
STIG-ID	WN19-CC-000450
STIG-LEGACY	SV-103357
STIG-LEGACY	V-93269
SWIFT-CSCV1	2.3
VULN-ID	V-205925

Assets

live-malware

WN19-DC-000010 - Windows Server 2019 must only allow administrators responsible for the domain controller to 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 using only accounts with the minimum level of authority necessary. Standard user accounts must not be members of the built-in Administrators group.

Solution

Configure the Administrators group to include only administrator groups or accounts that are responsible for the system.
Remove any standard user accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205738r958726_rule
STIG-ID	WN19-DC-000010
STIG-LEGACY	SV-103115
STIG-LEGACY	V-93027
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205738

Assets

live-malware

PASSED

WN19-DC-000020 - Windows Server 2019 Kerberos user logon restrictions must be enforced.

Info

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.4
800-171R3	03.05.04
800-53	IA-2(9)
800-53R5	IA-2(8)
CAT	II
CCI	CCI-001942
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	Windows_Server_2019_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(9)
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	AM18
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205702r1051071_rule
STIG-ID	WN19-DC-000020
STIG-LEGACY	SV-103529
STIG-LEGACY	V-93443
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205702

Assets

live-malware

PASSED

WN19-DC-000030 - Windows Server 2019 Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.

Info

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.4
800-171R3	03.05.04
800-53	IA-2(8)
800-53	IA-2(9)
800-53R5	IA-2(8)
CAT	II
CCI	CCI-001941
CCI	CCI-001942
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	Windows_Server_2019_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(8)
ITSG-33	IA-2(9)
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	AM18
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205703r1051072_rule
STIG-ID	WN19-DC-000030
STIG-LEGACY	SV-103531
STIG-LEGACY	V-93445
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205703

Assets

live-malware

PASSED

WN19-DC-000040 - Windows Server 2019 Kerberos user ticket lifetime must be limited to 10 hours or less.

Info

In Kerberos, there are two types of tickets: Ticket Granting Tickets (TGTs) and Service Tickets. Kerberos tickets have a limited lifetime so the time an attacker has to implement an attack is limited. This policy controls how long TGTs can be renewed. With Kerberos, the user's initial authentication to the domain controller results in a TGT, which is then used to request Service Tickets to resources. Upon startup, each computer gets a TGT before requesting a service ticket to the domain controller and any other computers it needs to access. For services that start up under a specified user account, users must always get a TGT first and then get Service Tickets to all computers and services accessed. Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.4
800-171R3	03.05.04
800-53	IA-2(8)
800-53	IA-2(9)
800-53R5	IA-2(8)
CAT	II
CCI	CCI-001941
CCI	CCI-001942
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	Windows_Server_2019_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(8)
ITSG-33	IA-2(9)
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	AM18
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205704r1051073_rule
STIG-ID	WN19-DC-000040
STIG-LEGACY	SV-103533
STIG-LEGACY	V-93447
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205704

Assets

live-malware

PASSED

WN19-DC-000050 - Windows Server 2019 Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.

Info

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.4
800-171R3	03.05.04
800-53	IA-2(8)
800-53	IA-2(9)
800-53R5	IA-2(8)
CAT	II
CCI	CCI-001941
CCI	CCI-001942
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	Windows_Server_2019_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(8)

ITSG-33	IA-2(9)
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	AM18
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205705r1051074_rule
STIG-ID	WN19-DC-000050
STIG-LEGACY	SV-103535
STIG-LEGACY	V-93449
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205705

Assets

live-malware

PASSED

WN19-DC-000060 - Windows Server 2019 computer clock synchronization tolerance must be limited to five minutes or less.

Info

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.4
800-171R3	03.05.04
800-53	IA-2(8)
800-53	IA-2(9)
800-53R5	IA-2(8)
CAT	II
CCI	CCI-001941
CCI	CCI-001942
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	Windows_Server_2019_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(8)
ITSG-33	IA-2(9)
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	AM18
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205706r1051075_rule
STIG-ID	WN19-DC-000060
STIG-LEGACY	SV-103537
STIG-LEGACY	V-93451
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205706

Assets

live-malware

PASSED

WN19-DC-000070 - Windows Server 2019 permissions on the Active Directory data files must only allow System and Administrators access.

Info

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

Solution

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

NT AUTHORITY\SYSTEM:(I)(F) BUILTIN\Administrators:(I)(F)

(I) - permission inherited from parent container (F) - full access

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205739r958726_rule
STIG-ID	WN19-DC-000070
STIG-LEGACY	SV-103117
STIG-LEGACY	V-93029
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205739

Assets

live-malware

PASSED

WN19-DC-000080 - Windows Server 2019 Active Directory SYSVOL directory must have the proper access control permissions.

Info

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

The SYSVOL directory contains public files (to the domain) such as policies and logon scripts. Data in shared subdirectories are replicated to all domain controllers in a domain.

Solution

Maintain the permissions on the SYSVOL directory. Do not allow greater than 'Read & execute' permissions for standard user accounts or groups. The defaults below meet this requirement:

C:\Windows\SYSVOL Type - 'Allow' for all Inherited from - 'None' for all

Principal - Access - Applies to

Authenticated Users - Read & execute - This folder, subfolder, and files Server Operators - Read & execute- This folder, subfolder, and files Administrators - Special - This folder only (Special = Basic Permissions: all selected except Full control) CREATOR OWNER - Full control - Subfolders and files only Administrators - Full control - Subfolders and files only SYSTEM - Full control - This folder, subfolders, and files

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205740r958726_rule
STIG-ID	WN19-DC-000080
STIG-LEGACY	SV-103119
STIG-LEGACY	V-93031
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205740

Assets

live-malware

PASSED

WN19-DC-000090 - Windows Server 2019 Active Directory Group Policy objects must have proper access control permissions.

Info

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems relying on the directory service.

For Active Directory (AD), the Group Policy objects require special attention. In a distributed administration model (i.e., help desk), Group Policy objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for Group Policy objects, this could allow an intruder to change the security policy applied to all domain client computers (workstations and servers).

Solution

Maintain the permissions on Group Policy objects to not allow greater than 'Read' and 'Apply group policy' for standard user accounts or groups. The default permissions below meet this requirement:

Authenticated Users - Read, Apply group policy, Special permissions

The special permissions for Authenticated Users are for Read-type Properties.

CREATOR OWNER - Special permissions SYSTEM - Read, Write, Create all child objects, Delete all child objects,

Special permissions Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special

permissions Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions

ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

Document any other access permissions that allow the objects to be updated with the ISSO.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205741r1081998_rule
STIG-ID	WN19-DC-000090
STIG-LEGACY	SV-103121
STIG-LEGACY	V-93033
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205741

Assets

live-malware

PASSED

WN19-DC-000100 - Windows Server 2019 Active Directory Domain Controllers Organizational Unit (OU) object must have the proper access control permissions.

Info

When Active Directory objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

The Domain Controllers OU object requires special attention as the Domain Controllers are central to the configuration and management of the domain. Inappropriate access permissions defined for the Domain Controllers OU could allow an intruder or unauthorized personnel to make changes that could lead to the compromise of the domain.

Solution

Limit the permissions on the Domain Controllers OU to restrict changes to System, Domain Admins, Enterprise Admins and Administrators.

The default permissions listed below satisfy this requirement.

Domains supporting Microsoft Exchange will have additional Exchange related permissions on the Domain Controllers OU. These may include some change related permissions.

CREATOR OWNER - Special permissions

SELF - Special permissions

Authenticated Users - Read, Special permissions

The special permissions for Authenticated Users are Read types.

SYSTEM - Full Control

Domain Admins - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions

Enterprise Admins - Full Control

Key Admins - Special permissions

Enterprise Key Admins - Special permissions

Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions

Pre-Windows 2000 Compatible Access - Special permissions

The special permissions for Pre-Windows 2000 Compatible Access are Read types.

ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205742r958726_rule
STIG-ID	WN19-DC-000100
STIG-LEGACY	SV-103123
STIG-LEGACY	V-93035
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

VULN-ID

V-205742

Assets
live-malware

PASSED

WN19-DC-000110 - Windows Server 2019 organization created Active Directory Organizational Unit (OU) objects must have proper access control permissions.

Info

When directory service database objects do not have appropriate access control permissions, it may be possible for malicious users to create, read, update, or delete the objects and degrade or destroy the integrity of the data. When the directory service is used for identification, authentication, or authorization functions, a compromise of the database objects could lead to a compromise of all systems that rely on the directory service.

For Active Directory, the OU objects require special attention. In a distributed administration model (i.e., help desk), OU objects are more likely to have access permissions changed from the secure defaults. If inappropriate access permissions are defined for OU objects, it could allow an intruder to add or delete users in the OU. This could result in unauthorized access to data or a denial of service (DoS) to authorized users.

Solution

Maintain the Allow type permissions on domain-defined OUs to be at least as restrictive as the defaults below.

Document any additional permissions above Read with the ISSO if an approved distributed administration model (help desk or other user support staff) is implemented.

CREATOR OWNER - Special permissions

Self - Special permissions

Authenticated Users - Read, Special permissions

The special permissions for Authenticated Users are Read type.

SYSTEM - Full Control

Domain Admins - Full Control

Enterprise Admins - Full Control

Key Admins - Special permissions

Enterprise Key Admins - Special permissions

Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions

Pre-Windows 2000 Compatible Access - Special permissions

The special permissions for Pre-Windows 2000 Compatible Access are for Read types.

ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205743r958726_rule
STIG-ID	WN19-DC-000110
STIG-LEGACY	SV-103125
STIG-LEGACY	V-93037
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205743

Assets

live-malware

PASSED

WN19-DC-000120 - Windows Server 2019 data files owned by users must be on a different logical partition from the directory server data files.

Info

When directory service data files, especially for directories used for identification, authentication, or authorization, reside on the same logical partition as user-owned files, the directory service data may be more vulnerable to unauthorized access or other availability compromises. Directory service and user-owned data files sharing a partition may be configured with less restrictive permissions in order to allow access to the user data.

The directory service may be vulnerable to a denial of service attack when user-owned files on a common partition are expanded to an extent preventing the directory service from acquiring more space for directory or audit data.

Solution

Move shares used to store files owned by users to a different logical partition than the directory server data files.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-205723r958524_rule
STIG-ID	WN19-DC-000120
STIG-LEGACY	SV-103621
STIG-LEGACY	V-93535
VULN-ID	V-205723

Assets

live-malware

PASSED

WN19-DC-000130 - Windows Server 2019 domain controllers must run on a machine dedicated to that function.

Info

Executing application servers on the same host machine with a directory server may substantially weaken the security of the directory server. Web or database server applications usually require the addition of many programs and accounts, increasing the attack surface of the computer.

Some applications require the addition of privileged accounts, providing potential sources of compromise. Some applications (such as Microsoft Exchange) may require the use of network ports or services conflicting with the directory server. In this case, non-standard ports might be selected, and this could interfere with intrusion detection or prevention services.

Solution

Remove additional roles or applications such as web, database, and email from the domain controller.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205695r958478_rule
STIG-ID	WN19-DC-000130

STIG-LEGACY	SV-103503
STIG-LEGACY	V-93417
SWIFT-CSCV1	2.3
VULN-ID	V-205695

Assets

live-malware

PASSED

WN19-DC-000140 - Windows Server 2019 must use separate, NSA-approved (Type 1) cryptography to protect the directory data in transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.

Info

Directory data that is not appropriately encrypted is subject to compromise. Commercial-grade encryption does not provide adequate protection when the classification level of directory data in transit is higher than the level of the network.

Solution

Configure NSA-approved (Type 1) cryptography to protect the directory data in transit for directory service implementations at a classified confidentiality level that transfer replication data through a network cleared to a lower level than the data.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205818r987791_rule
STIG-ID	WN19-DC-000140
STIG-LEGACY	SV-103599
STIG-LEGACY	V-93513
VULN-ID	V-205818

Assets

live-malware

PASSED

WN19-DC-000150 - Windows Server 2019 directory data (outside the root DSE) of a non-public directory must be configured to prevent anonymous access.

Info

To the extent that anonymous access to directory data (outside the root DSE) is permitted, read access control of the data is effectively disabled. If other means of controlling access (such as network restrictions) are compromised, there may be nothing else to protect the confidentiality of sensitive directory data.

Solution

Configure directory data (outside the root DSE) of a non-public directory to prevent anonymous access.

For AD, there are multiple configuration items that could enable anonymous access.

Changing the access permissions on the domain naming context object (from the secure defaults) could enable anonymous access. If the check procedures indicate this is the cause, the process that was used to change the permissions should be reversed. This could have been through the Windows Support Tools ADSI Edit console (adsiedit.msc).

The dsHeuristics option is used. This is addressed in check V-8555 in the AD Forest STIG.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205875r991589_rule
STIG-ID	WN19-DC-000150
STIG-LEGACY	SV-103359
STIG-LEGACY	V-93271
SWIFT-CSCV1	2.3

VULN-ID

V-205875

Assets

live-malware

PASSED

WN19-DC-000160 - Windows Server 2019 directory service must be configured to terminate LDAP-based network connections to the directory server after five minutes of inactivity.

Info

The failure to terminate inactive network connections increases the risk of a successful attack on the directory server. The longer an established session is in progress, the more time an attacker has to hijack the session, implement a means to passively intercept data, or compromise any protections on client access. For example, if an attacker gains control of a client computer, an existing (already authenticated) session with the directory server could allow access to the directory. The lack of confidentiality protection in LDAP-based sessions increases exposure to this vulnerability.

Solution

Configure the directory service to terminate LDAP-based network connections to the directory server after 5 minutes of inactivity.

Open an elevated 'Command prompt' (run as administrator).

Enter 'ntdsutil'.

At the 'ntdsutil:' prompt, enter 'LDAP policies'.

At the 'ldap policy:' prompt, enter 'connections'.

At the 'server connections:' prompt, enter 'connect to server [host-name]' (where [host-name] is the computer name of the domain controller).

At the 'server connections:' prompt, enter 'q'.

At the 'ldap policy:' prompt, enter 'Set MaxConnIdleTime to 300'.

Enter 'Commit Changes' to save.

Enter 'Show values' to verify changes.

Enter 'q' at the 'ldap policy:' and 'ntdsutil:' prompts to exit.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.13.9
800-171R3	03.13.09
800-53	SC-10
800-53R5	SC-10
CAT	III
CCI	CCI-001133
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.20
ITSG-33	SC-10
ITSG-33	SC-10a.
NESA	T2.3.8
NESA	T4.5.1
NESA	T5.5.1
RULE-ID	SV-205726r970703_rule
STIG-ID	WN19-DC-000160

STIG-LEGACY	SV-103595
STIG-LEGACY	V-93509
SWIFT-CSCV1	2.6
VULN-ID	V-205726

Assets

live-malware

PASSED

WN19-DC-000170 - Windows Server 2019 Active Directory Group Policy objects must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes Group Policy objects. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Configure the audit settings for Group Policy objects to include the following:

This can be done at the Policy level in Active Directory to apply to all group policies.

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Select 'Advanced Features' from the 'View' Menu.

Navigate to [Domain] >> System >> Policies in the left panel.

Right click 'Policies', select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button.

Select the 'Auditing' tab.

Type - Fail Principal - Everyone Access - Full Control Applies to - This object and all descendant objects or Descendant groupPolicyContainer objects

The three Success types listed below are defaults inherited from the Parent Object. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference.

Type - Success Principal - Everyone Access - Special (Permissions: Write all properties, Modify permissions; Properties: all 'Write' type selected) Inherited from - Parent Object Applies to - Descendant groupPolicyContainer objects

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - blank (Permissions: none selected; Properties: one instance - Write gPLink, one instance - Write gPOptions) Inherited from - Parent Object Applies to - Descendant Organization Unit Objects

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172

CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1

ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205785r958732_rule
STIG-ID	WN19-DC-000170
STIG-LEGACY	SV-103209
STIG-LEGACY	V-93121
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2

TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205785

Assets

live-malware

PASSED

WN19-DC-000180 - Windows Server 2019 Active Directory Domain object must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Ensure 'Advanced Features' is selected in the 'View' menu.

Select the domain being reviewed in the left pane.

Right-click the domain name and select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button and then the 'Auditing' tab.

Configure the audit settings for Domain object to include the following:

Type - Fail Principal - Everyone Access - Full Control Inherited from - None Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - (blank) Inherited from - None Applies to - Special

Type - Success Principal - Domain Users Access - All extended rights Inherited from - None Applies to - This object only

Type - Success Principal - Administrators Access - All extended rights Inherited from - None Applies to - This object only

Type - Success Principal - Everyone Access - Special Inherited from - None Applies to - This object only (Access - Special = Permissions: Write all properties, Modify permissions, Modify owner.)

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172

CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1

ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205786r958732_rule
STIG-ID	WN19-DC-000180
STIG-LEGACY	SV-103211
STIG-LEGACY	V-93123
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2

TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205786

Assets

live-malware

PASSED

WN19-DC-000190 - Windows Server 2019 Active Directory Infrastructure object must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Infrastructure object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Ensure 'Advanced Features' is selected in the 'View' menu.

Select the domain being reviewed in the left pane.

Right-click the 'Infrastructure' object in the right pane and select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button and then the 'Auditing' tab.

Configure the audit settings for Infrastructure object to include the following:

Type - Fail Principal - Everyone Access - Full Control Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Type - Success Principal - Everyone Access - Special Inherited from - None (Access - Special = Permissions: Write all properties, All extended rights, Change infrastructure master)

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - (blank) Inherited from - (CN of domain)

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6

ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205787r958732_rule
STIG-ID	WN19-DC-000190
STIG-LEGACY	SV-103213
STIG-LEGACY	V-93125
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1

VULN-ID

V-205787

Assets

live-malware

PASSED

WN19-DC-000200 - Windows Server 2019 Active Directory Domain Controllers Organizational Unit (OU) object must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the Domain Controller OU object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Ensure 'Advanced Features' is selected in the 'View' menu.

Select the 'Domain Controllers OU' under the domain being reviewed in the left pane.

Right-click the 'Domain Controllers OU' object and select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button and then the 'Auditing' tab.

Configure the audit settings for Domain Controllers OU object to include the following:

Type - Fail Principal - Everyone Access - Full Control Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Type - Success Principal - Everyone Access - Special Inherited from - None Applies to - This object only (Access - Special = Permissions: all create, delete and modify permissions)

Type - Success Principal - Everyone Access - Write all properties Inherited from - None Applies to - This object and all descendant objects

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - (blank) Inherited from - (CN of domain) Applies to - Descendant Organizational Unit objects

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234

CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3

ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205788r958732_rule
STIG-ID	WN19-DC-000200
STIG-LEGACY	SV-103215
STIG-LEGACY	V-93127
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

TBA-FIISB

45.1.1

VULN-ID

V-205788

Assets

live-malware

PASSED

WN19-DC-000210 - Windows Server 2019 Active Directory AdminSDHolder object must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the AdminSDHolder object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Ensure 'Advanced Features' is selected in the 'View' menu.

Select 'System' under the domain being reviewed in the left pane.

Right-click the 'AdminSDHolder' object in the right pane and select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button and then the 'Auditing' tab.

Configure the audit settings for AdminSDHolder object to include the following:

Type - Fail Principal - Everyone Access - Full Control Inherited from - None Applies to - This object only

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Type - Success Principal - Everyone Access - Special Inherited from - None Applies to - This object only (Access - Special = Write all properties, Modify permissions, Modify owner)

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - (blank) Inherited from - (CN of domain) Applies to - Descendant Organizational Unit objects

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6

ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205789r958732_rule
STIG-ID	WN19-DC-000210
STIG-LEGACY	SV-103217
STIG-LEGACY	V-93129
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1

VULN-ID

V-205789

Assets

live-malware

PASSED

WN19-DC-000220 - Windows Server 2019 Active Directory RID Manager\$ object must be configured with proper audit settings.

Info

When inappropriate audit settings are configured for directory service database objects, it may be possible for a user or process to update the data without generating any tracking data. The impact of missing audit data is related to the type of object. A failure to capture audit data for objects used by identification, authentication, or authorization functions could degrade or eliminate the ability to track changes to access policy for systems or data.

For Active Directory (AD), there are a number of critical object types in the domain naming context of the AD database for which auditing is essential. This includes the RID Manager\$ object. Because changes to these objects can significantly impact access controls or the availability of systems, the absence of auditing data makes it impossible to identify the source of changes that impact the confidentiality, integrity, and availability of data and systems throughout an AD domain. The lack of proper auditing can result in insufficient forensic evidence needed to investigate an incident and prosecute the intruder.

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

Solution

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Ensure 'Advanced Features' is selected in the 'View' menu.

Select 'System' under the domain being reviewed in the left pane.

Right-click the 'RID Manager\$' object in the right pane and select 'Properties'.

Select the 'Security' tab.

Select the 'Advanced' button and then the 'Auditing' tab.

Configure the audit settings for RID Manager\$ object to include the following:

Type - Fail Principal - Everyone Access - Full Control Inherited from - None

The success types listed below are defaults. Where Special is listed in the summary screens for Access, detailed Permissions are provided for reference. Various Properties selections may also exist by default.

Type - Success Principal - Everyone Access - Special Inherited from - None (Access - Special = Write all properties, All extended rights, Change RID master)

Two instances with the following summary information will be listed:

Type - Success Principal - Everyone Access - (blank) Inherited from - (CN of domain)

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)

CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)
CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6

ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3
NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205790r958732_rule
STIG-ID	WN19-DC-000220
STIG-LEGACY	SV-103219
STIG-LEGACY	V-93131
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1

VULN-ID

V-205790

Assets

live-malware

PASSED

WN19-DC-000230 - Windows Server 2019 must be configured to audit Account Management - Computer 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.

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.01
800-171R3	03.03.03a.
800-53	AC-2(4)
800-53	AU-12c.
800-53R5	AC-2(4)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000018
CCI	CCI-000172
CCI	CCI-001403
CCI	CCI-001404
CCI	CCI-001405
CCI	CCI-002130
CN-L3	7.1.3.2(d)
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.AC-4
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.AA-05
CSF2.0	PR.DS-10
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.16
ISO-27001-2022	A.5.18
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.12.4.1
ITSG-33	AC-2(4)
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5

NESA	T3.6.6
NESA	T5.2.2
NIAV2	AM9a
NIAV2	AM9b
NIAV2	AM9c
NIAV2	AM9d
NIAV2	AM9e
NIAV2	SM8
PCI-DSSV3.2.1	10.1
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205628r958368_rule
STIG-ID	WN19-DC-000230
STIG-LEGACY	SV-103073
STIG-LEGACY	V-92985
SWIFT-CSCV1	6.4
TBA-FIISB	36.2.3
TBA-FIISB	45.1.1
VULN-ID	V-205628

Assets

live-malware

PASSED

WN19-DC-000240 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access 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 Directory Service Access records events related to users accessing an Active Directory object.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205791r958732_rule
STIG-ID	WN19-DC-000240
STIG-LEGACY	SV-103221
STIG-LEGACY	V-93133
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205791

Assets

live-malware

PASSED

WN19-DC-000250 - Windows Server 2019 must be configured to audit DS Access - Directory Service Access 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 Directory Service Access records events related to users accessing an Active Directory object.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205792r958732_rule
STIG-ID	WN19-DC-000250
STIG-LEGACY	SV-103223
STIG-LEGACY	V-93135
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205792

Assets

live-malware

PASSED

WN19-DC-000260 - Windows Server 2019 must be configured to audit DS Access - Directory Service Changes 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 Directory Service Changes records events related to changes made to objects in Active Directory Domain Services.

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
800-171R3	03.01.07b.
800-171R3	03.03.03a.
800-53	AC-6(9)
800-53	AU-12c.
800-53R5	AC-6(9)
800-53R5	AU-12c.
CAT	II
CCI	CCI-000172
CCI	CCI-002234
CN-L3	7.1.3.2(b)
CN-L3	7.1.3.2(g)
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	8.1.4.2(d)
CN-L3	8.1.4.3(a)

CN-L3	8.1.10.6(a)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-4
CSF	PR.PT-1
CSF2.0	DE.CM-01
CSF2.0	DE.CM-03
CSF2.0	DE.CM-09
CSF2.0	PR.AA-05
CSF2.0	PR.PS-04
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
ISO-27001-2022	A.5.15
ISO-27001-2022	A.8.2
ISO-27001-2022	A.8.15
ISO-27001-2022	A.8.18
ISO/IEC-27001	A.12.4.1
ISO/IEC-27001	A.12.4.3
ITSG-33	AC-6
ITSG-33	AU-12c.
NESA	T3.6.2
NESA	T3.6.5
NESA	T3.6.6
NESA	T5.1.1
NESA	T5.2.2
NESA	T5.5.4
NESA	T7.5.3

NIAV2	AM1
NIAV2	AM23f
NIAV2	SM8
NIAV2	SS13c
NIAV2	SS15c
PCI-DSSV3.2.1	7.1.2
PCI-DSSV3.2.1	10.1
PCI-DSSV4.0	7.2.1
PCI-DSSV4.0	7.2.2
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-205793r958732_rule
STIG-ID	WN19-DC-000260
STIG-LEGACY	SV-103225
STIG-LEGACY	V-93137
SWIFT-CSCV1	5.1
SWIFT-CSCV1	6.4
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
TBA-FIISB	45.1.1
VULN-ID	V-205793

Assets

live-malware

PASSED

WN19-DC-000280 - Windows Server 2019 domain controllers must have a PKI server certificate.

Info

Domain controllers are part of the chain of trust for PKI authentications. Without the appropriate certificate, the authenticity of the domain controller cannot be verified. Domain controllers must have a server certificate to establish authenticity as part of PKI authentications in the domain.

Solution

Obtain a server certificate for the domain controller.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205645r958448_rule
STIG-ID	WN19-DC-000280
STIG-LEGACY	SV-103567
STIG-LEGACY	V-93481

VULN-ID

V-205645

Assets

live-malware

PASSED

WN19-DC-000290 - Windows Server 2019 domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority (ECA).

Info

A PKI implementation depends on the practices established by the Certificate Authority (CA) to ensure the implementation is secure. Without proper practices, the certificates issued by a CA have limited value in authentication functions. The use of multiple CAs from separate PKI implementations results in interoperability issues. If servers and clients do not have a common set of root CA certificates, they are not able to authenticate each other.

Solution

Obtain a server certificate for the domain controller issued by the DoD PKI or an approved ECA.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	I
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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-205646r958448_rule
STIG-ID	WN19-DC-000290
STIG-LEGACY	SV-103569

STIG-LEGACY

V-93483

VULN-ID

V-205646

Assets
live-malware

PASSED

WN19-DC-000300 - Windows Server 2019 PKI certificates associated with user accounts must be issued by a DoD PKI or an approved External Certificate Authority (ECA).

Info

A PKI implementation depends on the practices established by the Certificate Authority (CA) to ensure the implementation is secure. Without proper practices, the certificates issued by a CA have limited value in authentication functions.

Solution

Map user accounts to PKI certificates using the appropriate User Principal Name (UPN) for the network. See PKE documentation for details.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	I
CCI	CCI-000185
CSF	PR.AC-1
CSF2.0	PR.AA-01
CSF2.0	PR.AA-03
DISA_BENCHMARK	Windows_Server_2019_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-205647r958448_rule
STIG-ID	WN19-DC-000300
STIG-LEGACY	SV-103571

STIG-LEGACY

V-93485

VULN-ID

V-205647

Assets
live-malware

PASSED

WN19-DC-000310 - Windows Server 2019 Active Directory user accounts, including administrators, must be configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT) for user authentication.

Info

Smart cards such as the CAC support a two-factor authentication technique. This provides a higher level of trust in the asserted identity than use of the username and password for authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055, SRG-OS-000375-GPOS-00160

Solution

Configure all user accounts, including administrator accounts, in Active Directory to enable the option 'Smart card is required for interactive logon'.

Run 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc'):

Select the OU where the user accounts are located. (By default this is the Users node; however, accounts may be under other organization-defined OUs.)

Right-click the user account and select 'Properties'.

Select the 'Account' tab.

Check 'Smart card is required for interactive logon' in the 'Account Options' area.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.5.1
800-171	3.5.3
800-171R3	03.05.01a.
800-171R3	03.05.03
800-53	IA-2(3)
800-53	IA-2(4)
800-53	IA-2(11)
800-53R5	IA-2(1)
800-53R5	IA-2(2)
800-53R5	IA-2(6)
CAT	II
CCI	CCI-000767
CCI	CCI-000768
CCI	CCI-001948
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.1(d)
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	Windows_Server_2019_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(3)
ITSG-33	IA-2(4)
ITSG-33	IA-2(100)
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
PCI-DSSV3.2.1	8.3
PCI-DSSV3.2.1	8.3.1
PCI-DSSV3.2.1	8.3.2
PCI-DSSV4.0	8.4.1
PCI-DSSV4.0	8.4.3
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205701r1051070_rule
STIG-ID	WN19-DC-000310

STIG-LEGACY	SV-103527
STIG-LEGACY	V-93441
SWIFT-CSCV1	1.2
SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205701

Assets

live-malware

PASSED

WN19-DC-000320 - Windows Server 2019 domain controllers must require LDAP access signing.

Info

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

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205820r958908_rule
STIG-ID	WN19-DC-000320
STIG-LEGACY	SV-103631
STIG-LEGACY	V-93545
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205820

Assets

live-malware

PASSED

WN19-DC-000330 - Windows Server 2019 domain controllers must be configured to allow reset of machine account passwords.

Info

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

Solution

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

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205876r991589_rule
STIG-ID	WN19-DC-000330
STIG-LEGACY	SV-103361
STIG-LEGACY	V-93273
SWIFT-CSCV1	2.3
VULN-ID	V-205876

Assets

live-malware

PASSED

WN19-DC-000340 - Windows Server 2019 Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Access this computer from the network' right may access resources on the system, and this right must be limited to those requiring it.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Access this computer from the network' to include only the following accounts or groups:

- Administrators
- Authenticated Users
- Enterprise Domain Controllers

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205665r958472_rule
STIG-ID	WN19-DC-000340
STIG-LEGACY	SV-103083
STIG-LEGACY	V-92995
TBA-FIISB	31.1
VULN-ID	V-205665

Assets

live-malware

PASSED

WN19-DC-000350 - Windows Server 2019 Add workstations to domain user right must only be assigned to the Administrators group on domain controllers.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Add workstations to domain' right may add computers to a domain. This could result in unapproved or incorrectly configured systems being added to a domain.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Add workstations to domain' to include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205744r958726_rule
STIG-ID	WN19-DC-000350
STIG-LEGACY	SV-103127
STIG-LEGACY	V-93039
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205744

Assets

live-malware

PASSED

WN19-DC-000360 - Windows Server 2019 Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group on domain controllers.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the 'Allow log on through Remote Desktop Services' user right can access a system through Remote Desktop.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Allow log on through Remote Desktop Services' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205666r958472_rule
STIG-ID	WN19-DC-000360
STIG-LEGACY	SV-103085
STIG-LEGACY	V-92997
TBA-FIISB	31.1
VULN-ID	V-205666

Assets

live-malware

PASSED

WN19-DC-000370 - Windows Server 2019 Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Deny access to this computer from the network' user right defines the accounts that are prevented from logging on from the network. The Guests group must be assigned this right to prevent unauthenticated access.

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:

- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205667r958472_rule
STIG-ID	WN19-DC-000370
STIG-LEGACY	SV-103087
STIG-LEGACY	V-92999
TBA-FIISB	31.1
VULN-ID	V-205667

Assets

live-malware

PASSED

WN19-DC-000380 - Windows Server 2019 Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities.

The 'Deny log on as a batch job' user right defines accounts that are prevented from logging on to the system as a batch job, such as Task Scheduler.

The Guests group must be assigned to prevent unauthenticated access.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a batch job' to include the following:

- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205668r958472_rule
STIG-ID	WN19-DC-000380
STIG-LEGACY	SV-103089
STIG-LEGACY	V-93001
TBA-FIISB	31.1
VULN-ID	V-205668

Assets

live-malware

PASSED

WN19-DC-000390 - Windows Server 2019 Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Deny log on as a service' user right defines accounts that are denied logon as a service. Incorrect configurations could prevent services from starting and result in a denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a service' to include no entries (blank).

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205669r958472_rule
STIG-ID	WN19-DC-000390
STIG-LEGACY	SV-103091
STIG-LEGACY	V-93003
TBA-FIISB	31.1
VULN-ID	V-205669

Assets

live-malware

PASSED

WN19-DC-000391 - Windows Server 2019 must be configured for certificate-based authentication for domain controllers.

Info

Active Directory domain services elevation of privilege vulnerability could allow a user rights to the system, such as administrative and other high-level capabilities.

Solution

Configure the registry value.

Registry Hive: HKEY_LOCAL_MACHINE Registry Path: SYSTEM\CurrentControlSet\Services\Kdc

Value Name: StrongCertificateBindingEnforcement

Value Type: REG_DWORD Value: 0x00000001 (1) or 0x00000002 (2)

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-271428r1059563_rule
STIG-ID	WN19-DC-000391
TBA-FIISB	31.1
VULN-ID	V-271428

Assets

live-malware

PASSED

WN19-DC-000400 - Windows Server 2019 Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Deny log on locally' user right defines accounts that are prevented from logging on interactively. The Guests group must be assigned this right to prevent unauthenticated access.

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:
- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205670r958472_rule
STIG-ID	WN19-DC-000400
STIG-LEGACY	SV-103093
STIG-LEGACY	V-93005
TBA-FIISB	31.1
VULN-ID	V-205670

Assets

live-malware

PASSED

WN19-DC-000401 - Windows Server 2019 must be configured for named-based strong mappings for certificates.

Info

Weak mappings give rise to security vulnerabilities and demand hardening measures. Certificate names must be correctly mapped to the intended user account in Active Directory. A lack of strong name-based mappings allows certain weak certificate mappings, such as Issuer/Subject AltSecID and User Principal Names (UPN) mappings, to be treated as strong mappings.

Solution

Configure the policy value for Computer Configuration >> Administrative Template >> System >> KDC >> Allow name-based strong mappings for certificates to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-271429r1059566_rule
STIG-ID	WN19-DC-000401
TBA-FIISB	31.1
VULN-ID	V-271429

Assets

live-malware

PASSED

WN19-DC-000410 - Windows Server 2019 Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Deny log on through Remote Desktop Services' user right defines the accounts that are prevented from logging on using Remote Desktop Services. The Guests group must be assigned this right to prevent unauthenticated access.

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:
- Guests Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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-002314
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	Windows_Server_2019_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-205732r958672_rule
STIG-ID	WN19-DC-000410
STIG-LEGACY	SV-103051
STIG-LEGACY	V-92963
SWIFT-CSCV1	2.6
VULN-ID	V-205732

Assets

live-malware

PASSED

WN19-DC-000420 - Windows Server 2019 Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.

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 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 include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205745r958726_rule
STIG-ID	WN19-DC-000420
STIG-LEGACY	SV-103129
STIG-LEGACY	V-93041
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205745

Assets

live-malware

PASSED

WN19-DC-000430 - The password for the krbtgt account on a domain must be reset at least every 180 days.

Info

The krbtgt account acts as a service account for the Kerberos Key Distribution Center (KDC) service. The account and password are created when a domain is created and the password is typically not changed. If the krbtgt account is compromised, attackers can create valid Kerberos Ticket Granting Tickets (TGT).

The password must be changed twice to effectively remove the password history. Changing once, waiting for replication to complete and the amount of time equal to or greater than the maximum Kerberos ticket lifetime, and changing again reduces the risk of issues.

Solution

Reset the password for the krbtgt account a least every 180 days. The password must be changed twice to effectively remove the password history. Changing once, waiting for replication to complete and changing again reduces the risk of issues. Changing twice in rapid succession forces clients to reauthenticate (including application services) but is desired if a compromise is suspected.

PowerShell scripts are available to accomplish this such as at the following link:

<https://docs.microsoft.com/en-us/answers/questions/97108/resetting-the-krbtgt-account-password-in-a-domain.html>

All scripts should be tested.

Open 'Active Directory Users and Computers' (available from various menus or run 'dsa.msc').

Select 'Advanced Features' in the 'View' menu if not previously selected.

Select the 'Users' node.

Right-click on the krbtgt account and select 'Reset password'.

Enter a password that meets password complexity requirements.

Clear the 'User must change password at next logon' check box.

The system will automatically change this to a system-generated complex password.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205877r991589_rule
STIG-ID	WN19-DC-000430
STIG-LEGACY	SV-103299
STIG-LEGACY	V-93211
SWIFT-CSCV1	2.3
VULN-ID	V-205877

Assets

live-malware

PASSED

WN19-MS-000020 - Windows Server 2019 local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain-joined member servers.

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 local 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_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205715r958518_rule
STIG-ID	WN19-MS-000020
STIG-LEGACY	SV-103605
STIG-LEGACY	V-93519
VULN-ID	V-205715

Assets

live-malware

PASSED

WN19-MS-000030 - Windows Server 2019 local users on domain-joined member servers 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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205696r958478_rule
STIG-ID	WN19-MS-000030
STIG-LEGACY	SV-103505
STIG-LEGACY	V-93419

SWIFT-CSCV1

2.3

VULN-ID

V-205696

Assets

live-malware

PASSED

WN19-MS-000050 - Windows Server 2019 must limit the caching of logon credentials to four or less on domain-joined member servers.

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

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Interactive Logon: Number of previous logons to cache (in case Domain Controller is not available)' to '4' logons or less.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205906r991589_rule
STIG-ID	WN19-MS-000050
STIG-LEGACY	SV-103363
STIG-LEGACY	V-93275
SWIFT-CSCV1	2.3
VULN-ID	V-205906

Assets

live-malware

PASSED

WN19-MS-000100 - Windows Server 2019 'Deny log on as a service' user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts. No other groups or accounts must be assigned this right.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Deny log on as a service' user right defines accounts that are denied logon as a service. In an Active Directory Domain, denying logons to the Enterprise Admins and Domain Admins groups on lower-trust systems helps mitigate the risk of privilege escalation from credential theft attacks, which could lead to the compromise of an entire domain. Incorrect configurations could prevent services from starting and result in a denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Deny log on as a service' to include the following:

Domain systems:

- Enterprise Admins Group
- Domain Admins Group

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205674r958472_rule
STIG-ID	WN19-MS-000100
STIG-LEGACY	SV-103101
STIG-LEGACY	V-93013
TBA-FIISB	31.1
VULN-ID	V-205674

Assets

live-malware

PASSED

WN19-MS-000130 - Windows Server 2019 'Enable computer and user accounts to be trusted for delegation' user right must not be assigned to any groups or accounts on domain-joined member servers and standalone or nondomain-joined systems.

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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205748r958726_rule
STIG-ID	WN19-MS-000130
STIG-LEGACY	SV-103135
STIG-LEGACY	V-93047
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205748

Assets

live-malware

NULL

WN19-MS-000140 - Windows Server 2019 must be running Credential Guard on domain-joined member servers.

Info

Credential Guard uses virtualization-based security to protect data 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

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 article on Credential Guard system requirement can be found at the following link:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements>

Severity Override Guidance: The AO can allow the severity override if they have reviewed the overall protection provided to the affected servers that are not capable of complying with the Credential Guard requirement. Items that should be reviewed/considered for compliance or mitigation for non-Credential Guard compliance are:

The use of Microsoft Local Administrator Password Solution (LAPS) or similar products to control different local administrative passwords for all affected servers. This is to include a strict password change requirement (60 days or less).

....

Strict separation of roles and duties. Server administrator credentials cannot be used on Windows 10 desktop to administer it. Documentation of all exceptions should be supplied.

....

Use of a Privileged Access Workstation (PAW) and adherence to the Clean Source principle for administering affected servers.

....

Boundary Protection that is currently in place to protect from vulnerabilities in the network/servers.

....

Windows Defender rule block credential stealing from LSASS.exe is applied. This rule can only be applied if Windows Defender is in use.

....

The overall number of vulnerabilities that are unmitigated on the network/servers.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205907r991589_rule
STIG-ID	WN19-MS-000140
STIG-LEGACY	SV-103365
STIG-LEGACY	V-93277
SWIFT-CSCV1	2.3
VULN-ID	V-205907

Assets

live-malware

PASSED

WN19-SO-000010 - Windows Server 2019 must have the built-in guest account disabled.

Info

A system faces an increased vulnerability threat if the built-in guest account is not disabled. This is a known account that exists on all Windows systems and cannot be deleted. This account is initialized during the installation of the operating system with no password assigned.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205709r958504_rule
STIG-ID	WN19-SO-000010
STIG-LEGACY	SV-103583

STIG-LEGACY V-93497

SWIFT-CSCV1 2.8

VULN-ID V-205709

Assets

live-malware

'disabled'

WN19-SO-000020 - Windows Server 2019 must prevent local accounts with blank passwords from being used 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 should prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password does exist, enabling this setting will prevent network access, limiting the account to local console logon only.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205908r991589_rule
STIG-ID	WN19-SO-000020
STIG-LEGACY	SV-103367
STIG-LEGACY	V-93279
SWIFT-CSCV1	2.3
VULN-ID	V-205908

Assets

live-malware

WN19-SO-000030 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205909r991589_rule
STIG-ID	WN19-SO-000030
STIG-LEGACY	SV-103369
STIG-LEGACY	V-93281
SWIFT-CSCV1	2.3
VULN-ID	V-205909

Assets

live-malware

'admintest'

WN19-SO-000060 - Windows Server 2019 setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.

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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205821r958908_rule

STIG-ID	WN19-SO-000060
STIG-LEGACY	SV-103633
STIG-LEGACY	V-93547
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205821

Assets

live-malware

1

WN19-SO-000070 - Windows Server 2019 setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205822r958908_rule

STIG-ID	WN19-SO-000070
STIG-LEGACY	SV-103635
STIG-LEGACY	V-93549
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205822

Assets

live-malware

1

WN19-SO-000080 - Windows Server 2019 setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.

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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205823r958908_rule

STIG-ID	WN19-SO-000080
STIG-LEGACY	SV-103637
STIG-LEGACY	V-93551
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205823

Assets

live-malware

1

WN19-SO-000090 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205815r971545_rule
STIG-ID	WN19-SO-000090
STIG-LEGACY	SV-103541
STIG-LEGACY	V-93455
TBA-FIISB	27.1
VULN-ID	V-205815

Assets

live-malware

WN19-SO-000100 - Windows Server 2019 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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205911r991589_rule
STIG-ID	WN19-SO-000100
STIG-LEGACY	SV-103373
STIG-LEGACY	V-93285
SWIFT-CSCV1	2.3
VULN-ID	V-205911

Assets

WN19-SO-000110 - Windows Server 2019 must be configured to require a strong session key.

Info

A computer connecting to a domain controller will establish a secure channel. The secure channel connection may be subject to compromise, such as hijacking or eavesdropping, if strong session keys are not used to establish the connection. Requiring strong session keys enforces 128-bit encryption between systems.

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

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_Server_2019_V3R4_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	Windows_Server_2019_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-205824r958908_rule

STIG-ID	WN19-SO-000110
STIG-LEGACY	SV-103639
STIG-LEGACY	V-93553
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205824

Assets

live-malware

1

WN19-SO-000170 - Windows Server 2019 setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.

Info

The server message block (SMB) protocol provides the basis for many network operations. If this policy is enabled, the SMB client will request packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing.

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

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205826r958908_rule

STIG-ID	WN19-SO-000170
STIG-LEGACY	SV-103643
STIG-LEGACY	V-93557
SWIFT-CSCV1	2.1
TBA-FIISB	29.1
VULN-ID	V-205826

Assets

live-malware

1

WN19-SO-000180 - Windows Server 2019 unencrypted passwords must not be sent to third-party Server Message Block (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 determine 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_Server_2019_V3R4_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	Windows_Server_2019_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-205655r987796_rule
STIG-ID	WN19-SO-000180

STIG-LEGACY	SV-103555
STIG-LEGACY	V-93469
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-205655

Assets

live-malware

0

WN19-SO-000210 - Windows Server 2019 must not allow anonymous SID/Name translation.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205913r991589_rule
STIG-ID	WN19-SO-000210
STIG-LEGACY	SV-103377
STIG-LEGACY	V-93289
SWIFT-CSCV1	2.3
VULN-ID	V-205913

Assets

live-malware

'disabled'

WN19-SO-000220 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts.

Info

Anonymous enumeration of SAM accounts allows anonymous logon users (null session connections) to list all accounts names, thus providing a list of potential points to attack the system.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205914r991589_rule
STIG-ID	WN19-SO-000220
STIG-LEGACY	SV-103379
STIG-LEGACY	V-93291
SWIFT-CSCV1	2.3
VULN-ID	V-205914

Assets

live-malware

WN19-SO-000240 - Windows Server 2019 must be configured to prevent anonymous users from having the same permissions as the Everyone group.

Info

Access by anonymous users must be restricted. If this setting is enabled, anonymous users have the same rights and permissions as the built-in Everyone group. Anonymous users must not have these permissions or rights.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205915r991589_rule
STIG-ID	WN19-SO-000240
STIG-LEGACY	SV-103381
STIG-LEGACY	V-93293
SWIFT-CSCV1	2.3
VULN-ID	V-205915

Assets

live-malware

0

WN19-SO-000250 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares.

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SC-4
ITSG-33	SC-4a.
RULE-ID	SV-205725r958524_rule
STIG-ID	WN19-SO-000250
STIG-LEGACY	SV-103625
STIG-LEGACY	V-93539
VULN-ID	V-205725

Assets

live-malware

WN19-SO-000300 - Windows Server 2019 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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205654r1051063_rule

STIG-ID	WN19-SO-000300
STIG-LEGACY	SV-103553
STIG-LEGACY	V-93467
SWIFT-CSCV1	4.1
TBA-FIISB	26.1
VULN-ID	V-205654

Assets

live-malware

1

WN19-SO-000320 - Windows Server 2019 must be configured to at least negotiate signing for LDAP client signing.

Info

This setting controls the signing requirements for LDAP clients. This must be set to 'Negotiate signing' or 'Require signing', depending on the environment and type of LDAP server in use.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205920r991589_rule
STIG-ID	WN19-SO-000320
STIG-LEGACY	SV-103391
STIG-LEGACY	V-93303
SWIFT-CSCV1	2.3
VULN-ID	V-205920

Assets

live-malware

WN19-SO-000370 - Windows Server 2019 default permissions of global system objects must be strengthened.

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 Discretionary Access Control List (DACL) that specifies who can access the objects with what permissions. When this policy is enabled, the default DACL is stronger, allowing non-administrative users to read shared objects but not to modify shared objects they did not create.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205923r991589_rule
STIG-ID	WN19-SO-000370
STIG-LEGACY	SV-103397
STIG-LEGACY	V-93309
SWIFT-CSCV1	2.3
VULN-ID	V-205923

Assets

WN19-SO-000390 - Windows Server 2019 UIAccess applications must not be allowed to prompt for elevation without using 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 prevents User Interface Accessibility programs from disabling the secure desktop for elevation prompts.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205716r958518_rule
STIG-ID	WN19-SO-000390
STIG-LEGACY	SV-103607
STIG-LEGACY	V-93521
VULN-ID	V-205716

Assets

live-malware

0

WN19-SO-000420 - Windows Server 2019 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_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205718r958518_rule
STIG-ID	WN19-SO-000420
STIG-LEGACY	SV-103611
STIG-LEGACY	V-93525
VULN-ID	V-205718

Assets

live-malware

WN19-SO-000430 - Windows Server 2019 User Account Control (UAC) must only elevate UIAccess applications that are installed in secure locations.

Info

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_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205719r958518_rule
STIG-ID	WN19-SO-000430
STIG-LEGACY	SV-103613
STIG-LEGACY	V-93527
VULN-ID	V-205719

Assets

live-malware

WN19-SO-000440 - Windows Server 2019 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.

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

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_Server_2019_V3R4_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	Windows_Server_2019_STIG
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(d)
QCSC-V1	13.2
RULE-ID	SV-205813r1051085_rule
STIG-ID	WN19-SO-000440
STIG-LEGACY	SV-103521
STIG-LEGACY	V-93435
VULN-ID	V-205813

Assets

live-malware

WN19-SO-000450 - Windows Server 2019 User Account Control (UAC) must virtualize file and registry write failures to per-user locations.

Info

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_Server_2019_V3R4_STIG.zip

References

800-53	SC-3
800-53R5	SC-3
CAT	II
CCI	CCI-001084
DISA_BENCHMARK	Windows_Server_2019_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-205720r958518_rule
STIG-ID	WN19-SO-000450
STIG-LEGACY	SV-103615
STIG-LEGACY	V-93529
VULN-ID	V-205720

Assets

live-malware

WN19-UC-000010 - Windows Server 2019 must preserve zone information when saving attachments.

Info

Attachments from outside sources may contain malicious code. 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.

If this needs to be corrected, 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_Server_2019_V3R4_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	Windows_Server_2019_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-205924r991589_rule
STIG-ID	WN19-UC-000010
STIG-LEGACY	SV-103399
STIG-LEGACY	V-93311
SWIFT-CSCV1	2.3
VULN-ID	V-205924

Assets

live-malware

Compliant items:

HKU\S-1-5-21-259077641-1303433758-3492812687-500\Software\Microsoft\Windows\Currentversion
\Policies\Attachments -

WN19-UR-000010 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205749r958726_rule
STIG-ID	WN19-UR-000010
STIG-LEGACY	SV-103137
STIG-LEGACY	V-93049
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205749

Assets

live-malware

NULL

WN19-UR-000020 - Windows Server 2019 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 the 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_Server_2019_V3R4_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	Windows_Server_2019_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-205750r958726_rule
STIG-ID	WN19-UR-000020
STIG-LEGACY	SV-103139
STIG-LEGACY	V-93051
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205750

Assets

live-malware

NULL

WN19-UR-000050 - Windows Server 2019 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 include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205752r958726_rule
STIG-ID	WN19-UR-000050
STIG-LEGACY	SV-103143
STIG-LEGACY	V-93055
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205752

Assets

live-malware

'administrators'

WN19-UR-000060 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205753r958726_rule
STIG-ID	WN19-UR-000060
STIG-LEGACY	SV-103145
STIG-LEGACY	V-93057
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205753

Assets

live-malware

NULL

WN19-UR-000070 - Windows Server 2019 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 include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205754r958726_rule
STIG-ID	WN19-UR-000070
STIG-LEGACY	SV-103147
STIG-LEGACY	V-93059
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205754

Assets

live-malware

```
'service' && 'administrators' && 'network service' && 'local service'
```

WN19-UR-000080 - Windows Server 2019 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_Server_2019_V3R4_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	Windows_Server_2019_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-205755r958726_rule
STIG-ID	WN19-UR-000080
STIG-LEGACY	SV-103149
STIG-LEGACY	V-93061
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205755

Assets

live-malware

NULL

WN19-UR-000090 - Windows Server 2019 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 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 include only the following accounts or groups:

- Administrators

Systems that have the Hyper-V role will also have 'Virtual Machines' given this user right. If this needs to be added manually, enter it as 'NT Virtual Machine\Virtual Machines'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205756r958726_rule
STIG-ID	WN19-UR-000090
STIG-LEGACY	SV-103151
STIG-LEGACY	V-93063
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205756

Assets

live-malware

'administrators'

WN19-UR-000100 - Windows Server 2019 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 include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205757r958726_rule
STIG-ID	WN19-UR-000100
STIG-LEGACY	SV-103153
STIG-LEGACY	V-93065
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205757

Assets

live-malware

'administrators'

WN19-UR-000110 - Windows Server 2019 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 denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Force shutdown from a remote system' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205758r958726_rule
STIG-ID	WN19-UR-000110
STIG-LEGACY	SV-103155
STIG-LEGACY	V-93067
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205758

Assets

live-malware

'administrators'

WN19-UR-000120 - Windows Server 2019 Generate security audits user right must only be assigned to Local Service and Network Service.

Info

Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. The 'Generate security audits' user right specifies users and processes that can generate Security Log audit records, which must only be the system service accounts defined.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Generate security audits' to include only the following accounts or groups:

- Local Service
- Network Service

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205759r958726_rule
STIG-ID	WN19-UR-000120
STIG-LEGACY	SV-103157
STIG-LEGACY	V-93069
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205759

Assets

live-malware

```
'network service' && 'local service'
```

WN19-UR-000130 - Windows Server 2019 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 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 include only the following accounts or groups:

- Administrators
- Service
- Local Service
- Network Service

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205760r958726_rule
STIG-ID	WN19-UR-000130
STIG-LEGACY	SV-103159
STIG-LEGACY	V-93071
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205760

Assets

live-malware

```
'service' && 'administrators' && 'network service' && 'local service'
```

WN19-UR-000150 - Windows Server 2019 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 a user to load device drivers dynamically on a system. This could be used by an attacker to install malicious code.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Load and unload device drivers' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205762r958726_rule
STIG-ID	WN19-UR-000150
STIG-LEGACY	SV-103163
STIG-LEGACY	V-93075
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205762

Assets

live-malware

'administrators'

WN19-UR-000160 - Windows Server 2019 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 denial of service.

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_Server_2019_V3R4_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	Windows_Server_2019_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-205763r958726_rule
STIG-ID	WN19-UR-000160
STIG-LEGACY	SV-103165
STIG-LEGACY	V-93077
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205763

Assets

live-malware

NULL

WN19-UR-000170 - Windows Server 2019 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-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000063-GPOS-00032, SRG-OS-000337-GPOS-00129

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Manage auditing and security log' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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.
800-53	AU-12(3)
800-53R5	AU-9a.
800-53R5	AU-12b.
800-53R5	AU-12(3)
CAT	II
CCI	CCI-000162
CCI	CCI-000163
CCI	CCI-000164
CCI	CCI-000171
CCI	CCI-001914
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	Windows_Server_2019_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-12
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-205643r958434_rule
STIG-ID	WN19-UR-000170
STIG-LEGACY	SV-103285
STIG-LEGACY	V-93197
SWIFT-CSCV1	6.4
VULN-ID	V-205643

Assets

live-malware

'administrators'

WN19-UR-000180 - Windows Server 2019 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 denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Modify firmware environment values' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205764r958726_rule
STIG-ID	WN19-UR-000180
STIG-LEGACY	SV-103167
STIG-LEGACY	V-93079
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205764

Assets

live-malware

'administrators'

WN19-UR-000190 - Windows Server 2019 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. This could be used to delete volumes, resulting in data loss or a denial of service.

Solution

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> User Rights Assignment >> 'Perform volume maintenance tasks' to include only the following accounts or groups:

- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205765r958726_rule
STIG-ID	WN19-UR-000190
STIG-LEGACY	SV-103169
STIG-LEGACY	V-93081
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205765

Assets

live-malware

'administrators'

WN19-UR-000200 - Windows Server 2019 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 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 include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205766r958726_rule
STIG-ID	WN19-UR-000200
STIG-LEGACY	SV-103171
STIG-LEGACY	V-93083
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205766

Assets

live-malware

'administrators'

WN19-UR-000220 - Windows Server 2019 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 include only the following accounts or groups:
- Administrators

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205768r958726_rule
STIG-ID	WN19-UR-000220
STIG-LEGACY	SV-103175
STIG-LEGACY	V-93087
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205768

Assets

live-malware

'administrators'

Audits INFO,WARNING,ERROR

WN19-00-000010 - Windows Server 2019 users with Administrative privileges must have separate accounts for administrative duties and normal operational tasks.

Info

Using a privileged account to perform routine functions makes the computer vulnerable to malicious software inadvertently introduced during a session that has been granted full privileges.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Ensure each user with administrative privileges has a separate account for user duties and one for privileged duties.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205844r991589_rule
STIG-ID	WN19-00-000010
STIG-LEGACY	SV-103457
STIG-LEGACY	V-93369
SWIFT-CSCV1	2.3
VULN-ID	V-205844

Assets

live-malware

WN19-00-000030 - Windows Server 2019 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 require administrative accounts to not access the Internet or use applications such as email.

The policy should 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.

Whitelisting 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 a policy, at minimum, to prohibit administrative accounts from using applications that access the Internet, such as web browsers, or with potential Internet sources, such as email. Ensure the policy is enforced.

The organization may use technical means such as whitelisting to prevent the use of browsers and mail applications to enforce this requirement.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205845r991589_rule
STIG-ID	WN19-00-000030
STIG-LEGACY	SV-103293

STIG-LEGACY V-93205

SWIFT-CSCV1 2.3

VULN-ID V-205845

Assets

live-malware

WN19-00-000050 - Windows Server 2019 manually managed application account passwords must be at least 14 characters in length.

Info

Application/service account passwords must be of sufficient length to prevent being easily cracked. Application/service accounts that are manually managed must have passwords at least 14 characters in length.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Establish a policy that requires application/service account passwords that are manually managed to be at least 14 characters in length. Ensure the policy is enforced.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205661r1051068_rule
STIG-ID	WN19-00-000050
STIG-LEGACY	SV-103547
STIG-LEGACY	V-93461
SWIFT-CSCV1	4.1
TBA-FIISB	26.2.1
TBA-FIISB	26.2.4
VULN-ID	V-205661

Assets

live-malware

WN19-00-000070 - Windows Server 2019 shared user accounts must not be permitted.

Info

Shared accounts (accounts where two or more people log on with the same user identification) do not provide adequate identification and authentication. There is no way to provide for nonrepudiation or individual accountability for system access and resource usage.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Remove unapproved shared accounts from the system.

Document required shared accounts with the ISSO. Documentation must include the reason for the account, who has access to the account, and how the risk of using the shared account is mitigated to include monitoring account activity.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205699r958482_rule
STIG-ID	WN19-00-000070
STIG-LEGACY	SV-103523
STIG-LEGACY	V-93437
TBA-FIISB	35.1
TBA-FIISB	36.1
VULN-ID	V-205699

Assets

live-malware

```
' Name
----
admintest
DefaultAccount
Guest
WDAGUtilityAccount'
```

WN19-00-000080 - Windows Server 2019 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Info

Using an allowlist provides a configuration management method to allow 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 Server.

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 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_Server_2019_V3R4_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	Windows_Server_2019_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-205807r958808_rule
STIG-ID	WN19-00-000080
STIG-LEGACY	SV-103465
STIG-LEGACY	V-93379
SWIFT-CSCV1	2.3
TBA-FIISB	44.2.2
TBA-FIISB	49.2.3
VULN-ID	V-205807

Assets

live-malware

```
'<AppLockerPolicy Version="1" />'
```

WN19-00-000110 - Windows Server 2019 must use an anti-virus 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.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

If no anti-virus software is in use, install Windows Defender or third-party anti-virus.

Open 'PowerShell'.

Enter 'Install-WindowsFeature -Name Windows-Defender'.

For third-party anti-virus, install per anti-virus instructions and disable Windows Defender.

Open 'PowerShell'.

Enter 'Uninstall-WindowsFeature -Name Windows-Defender'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205850r991589_rule
STIG-ID	WN19-00-000110
STIG-LEGACY	SV-103305
STIG-LEGACY	V-93217
SWIFT-CSCV1	2.3
VULN-ID	V-205850

Assets

live-malware

```
'Status DisplayName
-----
Running Windows Defender Firewall
Running Windows Defender Advanced Threat Protection Service
Running Microsoft Defender Antivirus Network Inspection Service
Running Microsoft Defender Antivirus Service'
```

WN19-00-000120 - Windows Server 2019 must have a host-based intrusion detection or prevention system.

Info

A properly configured Host-based Intrusion Detection System (HIDS) or Host-based Intrusion Prevention System (HIPS) provides another level of defense against unauthorized access to critical servers. With proper configuration and logging enabled, such a system can stop and/or alert for many attempts to gain unauthorized access to resources.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Install a HIDS or HIPS on each server.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205851r991589_rule
STIG-ID	WN19-00-000120
STIG-LEGACY	SV-103307
STIG-LEGACY	V-93219
SWIFT-CSCV1	2.3
VULN-ID	V-205851

Assets

live-malware

WN19-00-000180 - Windows Server 2019 non-administrative accounts or groups must only have print permissions on printer shares.

Info

Windows shares are a means by which files, folders, printers, and other resources can be published for network users to access. Improper configuration can permit access to devices and data beyond a user's need.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure the permissions on shared printers to restrict standard users to only have Print permissions.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.02
800-53	AC-3
800-53R5	AC-3
CAT	III
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	Windows_Server_2019_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-205664r958472_rule
STIG-ID	WN19-00-000180
STIG-LEGACY	SV-103081
STIG-LEGACY	V-92993
TBA-FIISB	31.1
VULN-ID	V-205664

Assets

live-malware

WN19-00-000190 - Windows Server 2019 outdated or unused accounts must be removed or disabled.

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, disabled until needed.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Regularly review accounts to determine if they are still active. Remove or disable 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_Server_2019_V3R4_STIG.zip

References

800-171	3.5.5
800-171	3.5.6
800-171R3	03.05.05
800-53	IA-4e.
800-53R5	AC-2(3)(a)
CAT	II
CCI	CCI-000795
CCI	CCI-003627
CN-L3	7.1.2.7(b)
CSF	PR.AC-1
CSF2.0	PR.AA-01
DISA_BENCHMARK	Windows_Server_2019_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-4e.
PCI-DSSV3.2.1	8.1.4
PCI-DSSV4.0	8.2.6
QCSC-V1	5.2.2
QCSC-V1	13.2
RULE-ID	SV-205707r1051076_rule
STIG-ID	WN19-00-000190

STIG-LEGACY	SV-103543
-------------	-----------

STIG-LEGACY	V-93457
-------------	---------

SWIFT-CSCV1	5
-------------	---

VULN-ID	V-205707
---------	----------

Assets

live-malware

WN19-00-000220 - Windows Server 2019 system files must be monitored for unauthorized changes.

Info

Monitoring system files for changes against a baseline on a regular basis may help detect the possible introduction of malicious code on a system.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Monitor the system for unauthorized changes to system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) against a baseline on a weekly basis. This can be done with the use of various monitoring tools.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.4.3
800-171R3	03.04.03
800-53	CM-3(5)
800-53R5	CM-3(5)
CAT	II
CCI	CCI-001744
CN-L3	8.1.10.6(g)
CSF	DE.CM-1
CSF	DE.CM-7
CSF	PR.IP-1
CSF	PR.IP-3
CSF2.0	DE.CM-01
CSF2.0	DE.CM-09
CSF2.0	ID.RA-07
CSF2.0	PR.PS-01
DISA_BENCHMARK	Windows_Server_2019_STIG
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ISO-27001-2022	A.8.9
ISO-27001-2022	A.8.32
ISO-27001-2022	8.1
ISO-27001-2022	9.3.3
ISO/IEC-27001	A.12.1.2

ITSG-33	CM-3
NESA	T3.2.3
NESA	T3.3.2
NESA	T7.5.1
NESA	T7.6.1
NESA	T7.6.2
NESA	T7.6.3
NIAV2	CM1
NIAV2	CM1a
NIAV2	CM1b
NIAV2	CM1c
PCI-DSSV3.2.1	11.5
PCI-DSSV4.0	11.5.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	6.2
QCSC-V1	7.2
QCSC-V1	8.2.1
RULE-ID	SV-205803r958794_rule
STIG-ID	WN19-00-000220
STIG-LEGACY	SV-103291
STIG-LEGACY	V-93203
VULN-ID	V-205803

Assets

live-malware

WN19-00-000240 - Windows Server 2019 must have software certificate installation files removed.

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 or Adobe PreFlight certificate files.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205852r991589_rule
STIG-ID	WN19-00-000240
STIG-LEGACY	SV-103309
STIG-LEGACY	V-93221
SWIFT-CSCV1	2.3
VULN-ID	V-205852

Assets

live-malware

WN19-00-000250 - Windows Server 2019 systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Info

This requirement addresses protection of user-generated data as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure systems that require additional protections due to factors such as inadequate physical protection or sensitivity of the data to employ encryption to protect the confidentiality and integrity of all information at rest.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.13.16
800-171R3	03.13.08
800-53	SC-28
800-53	SC-28(1)
800-53R5	SC-28
800-53R5	SC-28(1)
CAT	I
CCI	CCI-001199
CCI	CCI-002475
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	Windows_Server_2019_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.
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-205727r958552_rule
STIG-ID	WN19-00-000250
STIG-LEGACY	SV-103601
STIG-LEGACY	V-93515
TBA-FIISB	28.1
VULN-ID	V-205727

Assets

live-malware

WN19-00-000260 - Windows Server 2019 must implement protection methods such as TLS, encrypted VPNs, or IPsec if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

Info

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to support transmission protection mechanisms such as TLS, encrypted VPNs, or IPsec.

Satisfies: SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure protection methods such as TLS, encrypted VPNs, or IPsec when the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.13.8
800-171R3	03.13.08
800-53	SC-8(2)
800-53R5	SC-8(2)
CAT	II
CCI	CCI-002420
CCI	CCI-002422
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	Windows_Server_2019_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(2)
ITSG-33	SC-9(2)
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-205829r958912_rule
STIG-ID	WN19-00-000260
STIG-LEGACY	SV-103629
STIG-LEGACY	V-93543

SWIFT-CSCV1

2.1

VULN-ID

V-205829

Assets

live-malware

WN19-00-000270 - Windows Server 2019 must have the roles and features required by the system documented.

Info

Unnecessary roles and features increase the attack surface of a system. Limiting roles and features of a system to only those necessary reduces this potential. The standard installation option (previously called Server Core) further reduces this when selected at installation.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Document the roles and features required for the system to operate. Uninstall any that are not required.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205677r958478_rule
STIG-ID	WN19-00-000270
STIG-LEGACY	SV-103467

STIG-LEGACY	V-93381
SWIFT-CSCV1	2.3
VULN-ID	V-205677

Assets		
live-malware		
'Display Name	Name	Install State
-----	----	-----
[X] File and Storage Services	FileAndStorage-Services	Installed
[X] Storage Services	Storage-Services	Installed
[X] .NET Framework 4.7 Features	NET-Framework-45-Fea...	Installed
[X] .NET Framework 4.7	NET-Framework-45-Core	Installed
[X] WCF Services	NET-WCF-Services45	Installed
[X] TCP Port Sharing	NET-WCF-TCP-PortShar...	Installed
[X] BitLocker Drive Encryption	BitLocker	Installed
[X] Enhanced Storage	EnhancedStorage	Installed
[X] System Data Archiver	System-DataArchiver	Installed
[X] Windows Defender Antivirus	Windows-Defender	Installed
[X] Windows PowerShell	PowerShellRoot	Installed
[X] Windows PowerShell 5.1	PowerShell	Installed
[X] Windows PowerShell ISE	PowerShell-ISE	Installed
[X] WoW64 Support	WoW64-Support	Installed
[X] XPS Viewer	XPS-Viewer	Installed'

WN19-00-000290 - Windows Server 2019 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where Endpoint Security Solution (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

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. The operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Install a 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_Server_2019_V3R4_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	Windows_Server_2019_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-205728r1000127_rule
STIG-ID	WN19-00-000290
STIG-LEGACY	SV-103653
STIG-LEGACY	V-93567
SWIFT-CSCV1	2.3

VULN-ID

V-205728

Assets

live-malware

WN19-00-000300 - Windows Server 2019 must automatically remove or disable temporary user accounts after 72 hours.

Info

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure temporary user accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date, under 'Account' properties.

Local accounts can be configured to expire with the command 'Net user [username] /expires:[mm/dd/yyyy]', where username is the name of the temporary user account.

Delete any temporary user accounts that are no longer necessary.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.01
800-53	AC-2(2)
800-53R5	AC-2(2)
CAT	II
CCI	CCI-000016
CN-L3	7.1.3.2(e)
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	Windows_Server_2019_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(2)
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205624r958364_rule
STIG-ID	WN19-00-000300
STIG-LEGACY	SV-103063
STIG-LEGACY	V-92975
VULN-ID	V-205624

Assets

live-malware

'Name : admintest
AccountExpires :

Name : DefaultAccount
AccountExpires :

Name : Guest
AccountExpires :

Name : WDAGUtilityAccount
AccountExpires :

WN19-00-000310 - Windows Server 2019 must automatically remove or disable emergency accounts after the crisis is resolved or within 72 hours.

Info

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Remove emergency administrator accounts after a crisis has been resolved or configure the accounts to automatically expire within 72 hours.

Domain accounts can be configured with an account expiration date, under 'Account' properties.

Local accounts can be configured to expire with the command 'Net user [username] /expires:[mm/dd/yyyy]', where username is the name of the temporary user account.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-171	3.1.1
800-171R3	03.01.01
800-53	AC-2(2)
800-53R5	AC-2(2)
CAT	II
CCI	CCI-001682
CN-L3	7.1.3.2(e)
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	Windows_Server_2019_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(2)
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
RULE-ID	SV-205710r958508_rule
STIG-ID	WN19-00-000310
STIG-LEGACY	SV-103065
STIG-LEGACY	V-92977
VULN-ID	V-205710

Assets

live-malware

WN19-00-000420 - Windows Server 2019 FTP servers must be configured to prevent anonymous logons.

Info

The FTP service allows remote users to access shared files and directories. Allowing anonymous FTP connections makes user auditing difficult.

Using accounts that have administrator privileges to log on to FTP risks that the userid and password will be captured on the network and give administrator access to an unauthorized user.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure the FTP service to prevent anonymous logons.

Open 'Internet Information Services (IIS) Manager'.

Select the server.

Double-click 'FTP Authentication'.

Select 'Anonymous Authentication'.

Select 'Disabled' under 'Actions'.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205853r991589_rule
STIG-ID	WN19-00-000420
STIG-LEGACY	SV-103311
STIG-LEGACY	V-93223

SWIFT-CSCV1

2.3

VULN-ID

V-205853

Assets

live-malware

WN19-00-000430 - Windows Server 2019 FTP servers must be configured to prevent access to the system drive.

Info

The FTP service allows remote users to access shared files and directories that could provide access to system resources and compromise the system, especially if the user can gain access to the root directory of the boot drive. NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure the FTP sites to allow access only to specific FTP shared resources. Do not allow access to other areas of the system.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205854r991589_rule
STIG-ID	WN19-00-000430
STIG-LEGACY	SV-103313
STIG-LEGACY	V-93225
SWIFT-CSCV1	2.3
VULN-ID	V-205854

Assets

live-malware

WN19-00-000450 - Windows Server 2019 must have orphaned security identifiers (SIDs) removed from user rights.

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 provided the target output to assist in reviewing 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_Server_2019_V3R4_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	Windows_Server_2019_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-205855r991589_rule
STIG-ID	WN19-00-000450
STIG-LEGACY	SV-103315
STIG-LEGACY	V-93227
SWIFT-CSCV1	2.3
VULN-ID	V-205855

Assets

live-malware

'Name	SID
admintest	S-1-5-21-259077641-1303433758-3492812687-500
DefaultAccount	S-1-5-21-259077641-1303433758-3492812687-503
Guest	S-1-5-21-259077641-1303433758-3492812687-501
WDAGUtilityAccount	S-1-5-21-259077641-1303433758-3492812687-504'

WN19-AU-000010 - Windows Server 2019 audit records must be backed up to a different system or media than the system being audited.

Info

Protection of log data includes assuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Establish and implement a process for backing up log data to another system or media other than the system being audited.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-53	AU-4(1)
800-53R5	AU-4(1)
CAT	II
CCI	CCI-001851
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Windows_Server_2019_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-205799r958754_rule
STIG-ID	WN19-AU-000010
STIG-LEGACY	SV-103271
STIG-LEGACY	V-93183
VULN-ID	V-205799

Assets

live-malware

WN19-AU-000020 - Windows Server 2019 must, at a minimum, offload audit records of interconnected systems in real time and offload standalone or nondomain-joined systems weekly.

Info

Protection of log data includes ensuring the log data is not accidentally lost or deleted. Audit information stored in one location is vulnerable to accidental or incidental deletion or alteration.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Configure the system to, at a minimum, offload audit records of interconnected systems in real time and offload standalone or nondomain-joined systems weekly.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_STIG.zip

References

800-53	AU-4(1)
800-53R5	AU-4(1)
CAT	II
CCI	CCI-001851
CSF	PR.DS-4
CSF	PR.PT-1
DISA_BENCHMARK	Windows_Server_2019_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-205843r959008_rule
STIG-ID	WN19-AU-000020
STIG-LEGACY	SV-103273
STIG-LEGACY	V-93185
VULN-ID	V-205843

Assets

live-malware

WN19-MS-000010 - Windows Server 2019 must only allow Administrators responsible for the member server or standalone or nondomain-joined system to 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 using only accounts with the minimum level of authority necessary. For domain-joined member servers, the Domain Admins group must be replaced by a domain member server administrator group (refer to AD.0003 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 built-in Administrators group.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure the local 'Administrators' group to include only administrator groups or accounts responsible for administration of the system.

For domain-joined member servers, replace the Domain Admins group with a domain member server administrator group.

Remove any standard user accounts.

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_Server_2019_V3R4_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	Windows_Server_2019_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-205746r958726_rule
STIG-ID	WN19-MS-000010
STIG-LEGACY	SV-103131
STIG-LEGACY	V-93043
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3
VULN-ID	V-205746

Assets

live-malware

```
'ADMINISTRATORS:
admintest'
```