

Tenable Vulnerability Management Report

Tenable Vulnerability Management

Mon, 15 Sep 2025 20:28:45 UTC

Table Of Contents

Remediations.....	10
•Suggested Remediations.....	11
Audits FAILED.....	12
•WN10-00-000031 - Windows 10 systems must use a BitLocker PIN for pre-boot authentication.....	13
•WN10-00-000032 - Windows 10 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication.....	15
•WN10-00-000090 - Accounts must be configured to require password expiration.....	17
•WN10-00-000145 - Data Execution Prevention (DEP) must be configured to at least OptOut.....	19
•WN10-00-000155 - The Windows PowerShell 2.0 feature must be disabled on the system.....	20
•WN10-00-000175 - The Secondary Logon service must be disabled on Windows 10.....	22
•WN10-AC-000005 - Windows 10 account lockout duration must be configured to 15 minutes or greater.....	24
•WN10-AC-000010 - The number of allowed bad logon attempts must be configured to 3 or less.....	26
•WN10-AC-000015 - The period of time before the bad logon counter is reset must be configured to 15 minutes.....	28
•WN10-AC-000020 - The password history must be configured to 24 passwords remembered.....	30
•WN10-AC-000030 - The minimum password age must be configured to at least 1 day.....	32
•WN10-AC-000035 - Passwords must, at a minimum, be 14 characters.....	34
•WN10-AC-000040 - The built-in Microsoft password complexity filter must be enabled.....	36
•WN10-AU-000005 - The system must be configured to audit Account Logon - Credential Validation failures.....	38
•WN10-AU-000010 - The system must be configured to audit Account Logon - Credential Validation successes.....	40
•WN10-AU-000050 - The system must be configured to audit Detailed Tracking - Process Creation successes.....	42
•WN10-AU-000060 - The system must be configured to audit Logon/Logoff - Group Membership successes.....	45
•WN10-AU-000081 - Windows 10 must be configured to audit Object Access - File Share failures.....	47
•WN10-AU-000082 - Windows 10 must be configured to audit Object Access - File Share successes.....	49
•WN10-AU-000085 - The system must be configured to audit Object Access - Removable Storage failures.....	51
•WN10-AU-000090 - The system must be configured to audit Object Access - Removable Storage successes.....	53
•WN10-AU-000107 - The system must be configured to audit Policy Change - Authorization Policy Change successes.....	55
•WN10-AU-000110 - The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.....	57
•WN10-AU-000115 - The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.....	60
•WN10-AU-000120 - The system must be configured to audit System - IPSec Driver failures.....	63
•WN10-AU-000500 - The Application event log size must be configured to 32768 KB or greater.....	65
•WN10-AU-000505 - The Security event log size must be configured to 1024000 KB or greater.....	66
•WN10-AU-000510 - The System event log size must be configured to 32768 KB or greater.....	67
•WN10-AU-000555 - Windows 10 must be configured to audit Other Policy Change Events Failures.....	68
•WN10-AU-000560 - Windows 10 must be configured to audit other Logon/Logoff Events Successes.....	70
•WN10-AU-000565 - Windows 10 must be configured to audit other Logon/Logoff Events Failures.....	72
•WN10-AU-000570 - Windows 10 must be configured to audit Detailed File Share Failures.....	74
•WN10-AU-000585 - Windows 10 must have command line process auditing events enabled for failures.....	76
•WN10-CC-000005 - Camera access from the lock screen must be disabled.....	78
•WN10-CC-000007 - Windows 10 must cover or disable the built-in or attached camera when not in use.....	80
•WN10-CC-000010 - The display of slide shows on the lock screen must be disabled.....	82
•WN10-CC-000020 - IPv6 source routing must be configured to highest protection.....	84
•WN10-CC-000025 - The system must be configured to prevent IP source routing.....	86

●WN10-CC-000030 - The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.....	88
●WN10-CC-000035 - The system must be configured to ignore NetBIOS name release requests except from WINS servers.....	90
●WN10-CC-000038 - WDigest Authentication must be disabled.....	92
●WN10-CC-000039 - Run as different user must be removed from context menus.....	94
●WN10-CC-000040 - Insecure logons to an SMB server must be disabled.....	96
●WN10-CC-000044 - Internet connection sharing must be disabled.....	97
●WN10-CC-000050 - Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.....	99
●WN10-CC-000052 - Windows 10 must be configured to prioritize ECC Curves with longer key lengths first.....	101
●WN10-CC-000060 - Connections to non-domain networks when connected to a domain authenticated network must be blocked.....	103
●WN10-CC-000066 - Command line data must be included in process creation events.....	105
●WN10-CC-000068 - Windows 10 must be configured to enable Remote host allows delegation of non-exportable credentials.....	107
●WN10-CC-000070 - Virtualization Based Security must be enabled on Windows 10 with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.....	109
●WN10-CC-000085 - Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.....	111
●WN10-CC-000090 - Group Policy objects must be reprocessed even if they have not changed.....	113
●WN10-CC-000100 - Downloading print driver packages over HTTP must be prevented.....	115
●WN10-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of providers.....	117
●WN10-CC-000110 - Printing over HTTP must be prevented.....	119
●WN10-CC-000120 - The network selection user interface (UI) must not be displayed on the logon screen.....	121
●WN10-CC-000145 - Users must be prompted for a password on resume from sleep (on battery).....	123
●WN10-CC-000150 - The user must be prompted for a password on resume from sleep (plugged in).....	124
●WN10-CC-000155 - Solicited Remote Assistance must not be allowed.....	125
●WN10-CC-000165 - Unauthenticated RPC clients must be restricted from connecting to the RPC server.....	126
●WN10-CC-000170 - The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.....	127
●WN10-CC-000175 - The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.....	128
●WN10-CC-000180 - Autoplay must be turned off for non-volume devices.....	130
●WN10-CC-000185 - The default autorun behavior must be configured to prevent autorun commands.....	131
●WN10-CC-000190 - Autoplay must be disabled for all drives.....	132
●WN10-CC-000195 - Enhanced anti-spoofing for facial recognition must be enabled on Window 10.....	134
●WN10-CC-000197 - Microsoft consumer experiences must be turned off.....	135
●WN10-CC-000200 - Administrator accounts must not be enumerated during elevation.....	137
●WN10-CC-000204 - If Enhanced diagnostic data is enabled it must be limited to the minimum required to support Windows Analytics.....	138
●WN10-CC-000205 - Windows Telemetry must not be configured to Full.....	140
●WN10-CC-000210 - The Windows Defender SmartScreen for Explorer must be enabled.....	142
●WN10-CC-000230 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for malicious websites in Microsoft Edge.....	144
●WN10-CC-000235 - Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for unverified files in Microsoft Edge.....	146
●WN10-CC-000238 - Windows 10 must be configured to prevent certificate error overrides in Microsoft Edge.....	148
●WN10-CC-000245 - The password manager function in the Edge browser must be disabled.....	149
●WN10-CC-000250 - The Windows Defender SmartScreen filter for Microsoft Edge must be enabled.....	150

•WN10-CC-000252 - Windows 10 must be configured to disable Windows Game Recording and Broadcasting....	152
•WN10-CC-000255 - The use of a hardware security device with Windows Hello for Business must be enabled.....	154
•WN10-CC-000260 - Windows 10 must be configured to require a minimum pin length of six characters or greater.....	156
•WN10-CC-000270 - Passwords must not be saved in the Remote Desktop Client.....	158
•WN10-CC-000275 - Local drives must be prevented from sharing with Remote Desktop Session Hosts.....	159
•WN10-CC-000280 - Remote Desktop Services must always prompt a client for passwords upon connection.....	160
•WN10-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.....	161
•WN10-CC-000290 - Remote Desktop Services must be configured with the client connection encryption set to the required level.....	163
•WN10-CC-000295 - Attachments must be prevented from being downloaded from RSS feeds.....	165
•WN10-CC-000305 - Indexing of encrypted files must be turned off.....	166
•WN10-CC-000310 - Users must be prevented from changing installation options.....	168
•WN10-CC-000315 - The Windows Installer Always install with elevated privileges must be disabled.....	170
•WN10-CC-000325 - Automatically signing in the last interactive user after a system-initiated restart must be disabled.....	172
•WN10-CC-000326 - PowerShell script block logging must be enabled on Windows 10.....	174
•WN10-CC-000327 - PowerShell Transcription must be enabled on Windows 10.....	176
•WN10-CC-000330 - The Windows Remote Management (WinRM) client must not use Basic authentication.....	178
•WN10-CC-000335 - The Windows Remote Management (WinRM) client must not allow unencrypted traffic.....	179
•WN10-CC-000345 - The Windows Remote Management (WinRM) service must not use Basic authentication....	180
•WN10-CC-000350 - The Windows Remote Management (WinRM) service must not allow unencrypted traffic....	182
•WN10-CC-000355 - The Windows Remote Management (WinRM) service must not store RunAs credentials....	183
•WN10-CC-000360 - The Windows Remote Management (WinRM) client must not use Digest authentication.....	184
•WN10-CC-000365 - Windows 10 must be configured to prevent Windows apps from being activated by voice while the system is locked.....	185
•WN10-CC-000370 - The convenience PIN for Windows 10 must be disabled.....	187
•WN10-CC-000385 - Windows Ink Workspace must be configured to disallow access above the lock.....	189
•WN10-CC-000391 - Internet Explorer must be disabled for Windows 10.....	191
•WN10-EP-000310 - Windows 10 Kernel (Direct Memory Access) DMA Protection must be enabled.....	192
•WN10-PK-000005 - The DoD Root CA certificates must be installed in the Trusted Root Store.....	193
•WN10-PK-000010 - The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.....	195
•WN10-PK-000015 - The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.....	197
•WN10-PK-000020 - The US DOD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.....	199
•WN10-SO-000005 - The built-in administrator account must be disabled.....	201
•WN10-SO-000025 - The built-in guest account must be renamed.....	203
•WN10-SO-000030 - Audit policy using subcategories must be enabled.....	204
•WN10-SO-000070 - The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.....	206
•WN10-SO-000075 - The required legal notice must be configured to display before console logon.....	208
•WN10-SO-000080 - The Windows dialog box title for the legal banner must be configured.....	210
•WN10-SO-000095 - The Smart Card removal option must be configured to Force Logoff or Lock Workstation....	212
•WN10-SO-000100 - The Windows SMB client must be configured to always perform SMB packet signing.....	213
•WN10-SO-000120 - The Windows SMB server must be configured to always perform SMB packet signing.....	216
•WN10-SO-000150 - Anonymous enumeration of shares must be restricted.....	219

•WN10-SO-000167 - Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.....	220
•WN10-SO-000180 - NTLM must be prevented from falling back to a Null session.....	222
•WN10-SO-000185 - PKU2U authentication using online identities must be prevented.....	223
•WN10-SO-000190 - Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.....	224
•WN10-SO-000205 - The LanMan authentication level must be set to send NTLMv2 response only, and to refuse LM and NTLM.....	226
•WN10-SO-000215 - The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.....	228
•WN10-SO-000220 - The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.....	230
•WN10-SO-000230 - The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.....	232
•WN10-SO-000245 - User Account Control approval mode for the built-in Administrator must be enabled.....	234
•WN10-SO-000250 - User Account Control must, at minimum, prompt administrators for consent on the secure desktop.....	235
•WN10-SO-000255 - User Account Control must automatically deny elevation requests for standard users.....	236
•WN10-SO-000280 - Passwords for enabled local Administrator accounts must be changed at least every 60 days.....	237
•WN10-UR-000010 - The Access this computer from the network user right must only be assigned to the Administrators and Remote Desktop Users groups.....	239
•WN10-UR-000025 - The Allow log on locally user right must only be assigned to the Administrators and Users groups.....	241
•WN10-UR-000030 - The Back up files and directories user right must only be assigned to the Administrators group.....	243
•WN10-UR-000035 - The Change the system time user right must only be assigned to Administrators and Local Service and NT SERVICE\autotimesvc.....	245
•WN10-UR-000070 - The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.....	247
•WN10-UR-000085 - The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.....	249
•WN10-UR-000090 - The Deny log on through Remote Desktop Services user right on Windows 10 workstations must at a minimum be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.....	251
•WN10-UR-000160 - The Restore files and directories user right must only be assigned to the Administrators group.....	254

Audits SKIPPED..... 256

Audits PASSED..... 257

•DISA_Microsoft_Windows_10_STIG_v3r4.audit from DISA Microsoft Windows 10 STIG v3r4.....	258
•WN10-00-000005 - Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.....	259
•WN10-00-000015 - Windows 10 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.....	260
•WN10-00-000020 - Secure Boot must be enabled on Windows 10 systems.....	261
•WN10-00-000040 - Windows 10 systems must be maintained at a supported servicing level.....	262
•WN10-00-000045 - The Windows 10 system must use an anti-virus program.....	264
•WN10-00-000050 - Local volumes must be formatted using NTFS.....	266
•WN10-00-000075 - Only accounts responsible for the backup operations must be members of the Backup Operators group.....	268
•WN10-00-000080 - Only authorized user accounts must be allowed to create or run virtual machines on Windows 10 systems.....	270
•WN10-00-000085 - Standard local user accounts must not exist on a system in a domain.....	272