MICROSOFT WINDOWS 2012/2012 R2 DOMAIN CONTROLLER (DC) STIG REVISION HISTORY

Version 3, Release 6

11 May 2023

Developed by DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V3R6	- Windows 2012/2012 R2 DC STIG, V3R5	- WN12-00-000018 - In Check and Fix, revised link for AppLocker Deployment Guide. In Check, removed wording "This is applicable to unclassified systems. For other systems, this is NA." Replaced "whitelist" with "allowlist." - WN12-AU-000030 - Removed requirement to audit Logon/Logoff - Account Lockout successes. - WN12-AU-000036-DC - Removed requirement to audit DS Access - Directory Service Changes failures. - WN12-GE-000017 - Revised Check to remove ESS (MACC). - WN12-PK-000001 - Revised Fix to add PKI link for DOD certificates. - WN12-PK-000003, WN12-PK-000004 - Revised Check and Fix to reflect updated certificates and added PKI link for DOD certificates to Fix. - Some Rule IDs updated due to changes in content management system.	11 May 2023
V3R5	- Windows 2012/2012 R2 DC STIG, V3R4	- WN12-CC-000069 - Updated hyperlink in Check and Fix text. - WN12-GE-000016 - Removed from Check text "Domain accounts requiring smart card (CAC/PIV) may also be excluded". - WN12-GE-000017 - Updated Check text: "A properly configured McAfee Application Control and Change Control (MACC) module will meet the requirement for file integrity checking." - Some Rule IDs and CCIs updated due to minor changes in content management system.	14 November 2022
V3R4	- Windows 2012/2012 R2 DC STIG, V3R3	- WN12-PK-000001, WN12-PK-000003 - Removed all deprecated DOD Root CA 2 references.	31 May 2022
V3R3	- Windows 2012/2012	- The last six digits in all SV numbers have changed.	01 November 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	R2 DC STIG, V3R2	- WN12-00-000007 - Updated Vul Discussion/Fix to highly recommend use of LAPS, and AO can approve other solutions. - WN12-CC-000007, WN12-CC-000008, WN12-CC-000009, WN12-CC-000010 - Due to DOD migration to IPv6, removed requirement to disable IPv6. - WN12-GE-000017, WN12-GE-000022, WN12-GE-000023 - Replaced HBSS references with Endpoint Security Solution. - WN12-GE-000019 - Removed this requirement to mandate McAfee Agent.	
V3R2	- Windows 2012/2012 R2 DC DC STIG, V3R1	- WN12-AD-000002-DC - Removed the File Explorer option from the Check. This option could impact SYS volumes properties and cause corruption. Added a finding statement to the Check. - WN12-AD-000005-DC, WN12-AD-000012-DC, WN12-AD-000013-DC, WN12-PK-000006-DC, WN12-SO-000036, WN12-UR-000002-DC - Added back MISC Data - Severity Override Guidance. - WN12-GE-000023 - Removed HBSS wording. Updated Check and Fix and added Note section.	04 May 2021
V3R1	- Windows 2012/2012 R2 DC STIG, V2R21	- DISA migrated the STIG to a new content management system, which renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V2R21 to V3R1. - WN12-CC-000131 - Removed requirement that remote Desktop Services must limit users to one remote session. - WN12-GE-000017 - Updated check text with, "A properly configured and approved DOD HBSS solution that supports a File Integrity Monitor (FIM) module will meet the requirement for file integrity checking". - WN12-PK-000001 - Removed "not a finding" wording.	13 November 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- WN12-PK-000003, WN12-PK-000004 - Removed "If an expired certificate ("Valid to" date)" wording; updated identified certificates.	
V2R21	- Windows 2012/2012 R2 DC STIG, V2R20	- V-102619 - In Check text, separated registry settings. In Fix text, added >> Explorer Frame Pane.	17 June 2020
V2R20	- Windows 2012/2012 R2 DC STIG, V2R19	- V-1081 - Added CSV (Cluster Share Volumes) wording to Check Text. - V-14229 - Updated registry to Value: 00. - V-102619 - Added requirement: The Windows Explorer Preview pane must be disabled for Windows Server 2012 DC.	15 May 2020
V2R19	- Windows 2012/2012 R2 DC STIG, V2R18	- V-91777 - Change in discussion: 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."	24 January 2020
V2R18	- Windows 2012/2012 R2 DC STIG, V2R17	- V-1135 - Modified check text (exclude Microsoft Print to PDF and Microsoft XPS Document Writer, which do not support sharing).	25 October 2019
V2R17	- Windows 2012/2012 R2 DC STIG, V2R16	- V-3376 - Removed Storage of Passwords and Credentials requirement. - V-7002 - Updated requirement with note excluding Trust Domain Objects (TDOs). - V-15823 - Added note to requirement regarding Adobe Preflight certificate files. - V-36707 - Updated requirement with applicability note for unclassified systems. - V-36734 - Modified Check and Fix text to require "DOD approved HBSS software". - V-80475 - Updated requirement to remove extra space from registry path.	26 July 2019
V2R16	- Windows 2012/2012	- V-15713 - Removed Defender - SpyNet Reporting requirement.	26 April 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	R2 DC STIG, V2R15	- V-32274 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Added new certificate. Removed expired certificates. - V-40237 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Removed expired certificate.	
V2R15	- Windows 2012/2012 R2 DC STIG, V2R14	- V-91777 – Added KRBTGT password reset requirement.	08 February 2019
V2R14	- Windows 2012/2012 R2 DC STIG, V2R13	- V78057, V-78059, V-78061, and V-78063 – Corrected group policy path. - V-21954 - Removed RC4_HMAC_MD5 as an allowed option. - V-12780, V-26476, V-26497, V-26501, and V-26503 - Removed user right requirement to align with Windows 2016 STIG. - V-26469, V- 26478, V-26481, V-26482, V-26488, V-26493, V-26496, V-26498, V-26499, and V-26500 - Updated Rule Title to specific requirement. - V-1102, V-18010, V-26472, V-26474, V-26479, V-26480, V-26489, V-26490, V-26492, V-26494, V-26504, and V-26506 - Updated Rule Title to specific requirement. Moved Severity Override to Check section. - V-36773 - Updated to clarify "0" is not allowed.	26 October 2018
V2R13	- Windows 2012/2012 R2 DC STIG, V2R12	- V-3472 - Updated to use w32tm command to determine effective setting. - V-32272 - Updated with additional certificate. Added certificate expiration dates for reference. - V-32274 - Added certificate expiration dates for reference. - V-36707 - Updated SmartScreen requirement to allow either enabled option.	27 July 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-40237 - Updated with additional certificate. Added certificate expiration dates for reference. - V-57637 - Updated link to referenced NSA document. - V-80473 - Added requirement for PowerShell to be updated to version that supports script block logging. - V-80475 - Added requirement for PowerShell script block logging to be enabled. - V-80477 - Added requirement to verify PowerShell 2.0 has not been installed. **Windows 2012 and 2012 R2 DC Benchmark, V2R13:** - V-32272 - Updated DOD Root CA OVAL content to include additional certificate. - V-36707 - Updated Windows SmartScreen requirement OVAL content to allow for either enabled option. - V-36773 - Updated Machine Inactivity OVAL content to ensure a value of "0" will result in a finding. - V-40237 - Updated DOD CCEB Interoperability Root CA OVAL content to include additional certificate. - V-80473 - Create new OVAL to check that PowerShell V4 or v5.x is installed. - V-80477 - Create new OVAL to check that PowerShell v2 is not installed.	
V2R12	- Windows 2012/2012 R2 DC STIG, V2R11	- V-1072 - Updated allowed exceptions note. - V-26534 - Removed Other Account Management failure event audit requirement as NA. - V-26536 - Removed Security Group Management failure event audit requirement as NA. - V-26556 - Removed Security System Extension failure event audit requirement as NA.	27 April 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-39325 - Updated group policy object auditing method and scope. - V-40175 - Removed antivirus signature requirement, addressed by AV product STIGs. **Windows 2012 and 2012 R2 DC Benchmark, V2R12:** - V-26534, V-26536, and V-26556 - Disabled OVAL due to STIG rule removal.	
V2R11	- Windows 2012/2012 R2 DC STIG, V2R10	- V-6840 and V-7002 - Updated to use Windows queries instead of DumpSec application. - V-14225 - Updated to use Windows queries instead of DumpSec application. - V-15823 - Clarified noted exceptions. - V-26531 - Updated Audit Computer Account Management Success to apply to Domain Controllers only. - V-26532 - Removed requirement Audit Computer Account Management Failures to align with Windows 2016 STIG. - V-26554 - Removed requirement Audit Security State Change Failures to align with Windows 2016 STIG. - V-36662 - Updated to use Windows queries instead of DumpSec application. - V-36707 - Changed SmartScreen requirement to align with other Windows STIGs - Enabled and CAT II. - V-57635 - Removed requirement Audit Authorization Policy Change Failures to align with Windows 2016 STIG. - V-78057 - Added Audit Account Lockout Successes to align with Windows 2016 STIG. - V-78059 - Added Audit Account Lockout Failures to align with Windows 2016 STIG. - V-78061 - Added Audit Other System Events Successes to align with Windows 2016 STIG.	26 January 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-78063 - Added Audit Other System Events Failures to align with Windows 2016 STIG. **Windows 2012 and 2012 R2 DC Benchmark, V2R11:** - V-26532 and V-26554 - Removed OVAL content, requirement removed from the manual STIG. - V-36707 - Updated the OVAL content for the SmartScreen requirement in conjunction with the change to the manual STIG. - V-57633 - Updated OVAL content for the Audit Authorization Policy Change (Success). - V-57635 - Removed OVAL content, requirement removed from the manual STIG. - V-78057 - Added new OVAL content for the Audit Account Lockout (Success). - V-78059 - Added new OVAL content for the Audit Account Lockout (Failure). - V-78061 - Added new OVAL content for the Audit Other System Events (Success). - V-78063 - Added new OVAL content for the Audit Other System Events (Failure).	
V2R10	- Windows 2012/2012 R2 DC STIG, V2R9	- The SecGuide custom admin template files have been updated to include additional configuration settings. - V-1074 - Removed specific antivirus product referenced. - V-1089 - Removed short version of banner text as NA. - V-26683 - Clarified various formats may exist for individual identifiers. - V-32272 - Clarified details apply to unclassified systems, refers to PKE documentation for other systems. - V-39332 - Clarified changes from schema update to support Exchange are not a finding. - V-43239 - Changed requirement to enable command line data to be included in process creation events.	27 October 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-57653 - Clarified applicability of requirement for temporary accounts. - V-57655 - Clarified applicability of requirement for emergency administrative accounts. - V-73519 - Updated Fix to use custom administrative template for configuration. - V-73523 - Modified Check to only be a finding if SMBV2 is found. Updated Fix to use custom administrative template for configuration. - V-73805 - Updated to allow alternate method for disabling SMBV2. - V-75915 - Added requirement for unresolved SIDs found on user rights. - Removed the following requirements that provide minimal security benefit: V-36774 - Require a specific screen saver. V-36775 - Prevent screen saver change. V-26475 - Bypass traverse checking user right. V-26477 - Change the time zone user right. V-26505 - Shut down the system user right. **Windows 2012 and 2012 R2 DC Benchmark, V2R10:** - Removed OVAL content for the following as requirement has been removed from the STIG: V-26475, V-26477, and V-26505. - V-32282 - Added OVAL content to the benchmark. - V-43239 - Updated the OVAL content for change in requirement. - V-73519 - Updated the OVAL content for SMBV2 Server requirement to pass on Windows Server 2012 R2. - V-73523 - Updated the OVAL content for SMBV2 Client requirement to pass on Windows Server 2012 R2. Updated DependOnService to be a finding only if SMBV2 is found and not specifically for other defaults.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-73805 - Updated the OVAL content for SMBV2 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.	
V2R9	- Windows 2012/2012 R2 DC STIG, V2R8	- V-1081 - Updated to include ReFS as an acceptable disk format. - V-1098 - Updated reset account lockout counter to 15 minutes or greater. - V-1099 - Updated account lockout duration to 15 minutes or greater. - V-1112 - Corrected typo referring to built-in admin account as disabled. - V-1120 and V-1121 - Updated Check to more accurately verify FTP configuration. - V-14243 - Updated Rule Title to more accurately reflect requirement. - V-26602 - Clarified Rule Title; service must be disabled unless required. - V-36451 - Clarified requirement; policy required, technical means to enforce. **Windows 2012 and 2012 R2 DC Benchmark, V2R9:** - V-1081 - Updated OVAL to reflect STIG changes that allow for ReFS. - V-1098 - Updated OVAL content for reset account lockout counter change to 15 minutes or greater. - V-1099 - Updated OVAL content for account lockout duration change to 15 minutes. - V-1152 - Added OVAL to check permissions on Winreg registry key. - V-26070 - Added OVAL to check permissions on Winlogon registry key. - V-26580 - Updated the OVAL content to allow Security Log maximum size to be 196608 KB or more.	28 July 2017
V2R8	- Windows 2012/2012 R2 DC STIG, V2R7	- V-1074 - Updated requirement consistent with other Windows STIGs. Changed STIG ID.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1152 - Clarified permissions must be at least as restrictive as defaults. - V-15505 - Clarified versions of service being verified. - V-8316 and V-26070 - Clarified permissions must be at least as restrictive as defaults. - V-26683 - Updated Check and Fix to align with PKE guidance for mapping accounts. - V-40175 - Updated to require configuration of daily checks for signatures as well as a maximum age of one week. Changed STIG ID. - V-73519 and V-73523 - Added requirement to disable Server Message Block (SMB) V2 on the Windows 2012 SMB server. - V-73805 - Added requirement to disable Server Message Block (SMB) V2 on Windows 2012 R2. **Windows 2012 and 2012 R2 DC Benchmark, V2R8:** - V-8316 - Updated the OVAL content to refine the pattern match for NTDS log files. - V-15505 - Added OVAL to check if one of the supported versions of the McAfee agents is installed and running. - V-73519 - Added OVAL to check if the SMBV2 protocol for the SMB server is disabled for Windows 2012. - V-73523 - Added OVAL to check if the SMBV2 protocol for the SMB client is disabled for Windows 2012. - V-73805 - Added OVAL to check if the SMB 1.0/CIFS File Sharing Support feature is disabled in Windows 2012 R2.	
V2R7	- Windows 2012/2012 R2 DC STIG, V2R6	- V-26496 - Updated to include application exception. - V-32274 - Updated expired certificate with replacement. - V-72753 - Added requirement to disable WDigest.	27 January 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Removed Error Reporting requirements: V-15714, V-15715, V-15717, V-56511, V-57453, V-57455, V-57457, V-57459, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, and V-57479. - The following were removed by DOD Consensus: V-1158, V-1159, V-3457, V-3458, V-4446, V-15719, V-16005, V-26471, V-26491, V-26495, and V-36772. **Windows 2012 and 2012 R2 DC Benchmark, V2R7:** - V-8316 - Updated OVAL to handle different tools' ways of handling case sensitivity. - V-32274 - Updated OVAL with new certificate information. - Disabled the following rules in OVAL in conjunction with the removal of the requirements from the manual STIG: V-1158, V-1159, V-3457, V-3458, V-15714, V-15715, V-15717, V-15719, V-16005, V-26471, V-26491, V-26495, V-36772, V-56511, V-57453, V-57455, V-57457, V-57459, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, and V-57479.	
V2R6	- Windows 2012/2012 R2 DC STIG, V2R5	- V-1163 and V-1164 - Removed data in False Positive field, duplicated in Check. - V-15505 - Updated for v5 of McAfee agent. - V-32272 and V-32274 - Updated PKE related requirement with current certificates. - V-3245 - Removed data in False Positive field, duplicated in Check. - V-3383 - Removed data in Potential Impacts field, duplicated in Check. - V-36663 and V-36664 - Removed BIOS related requirement as outside of OS scope. - V-36667 and V-36668 - Clarified for virtual machines and systems with network attached storage.	28 October 2016

11

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-40193 - Removed requirement for virtual machine asset registration. - V-40195 - Removed BIOS related requirement as outside of OS scope. - V-40237 - Updated PKE related requirement with current certificates. - V-56511 - Clarified Windows Error Reporting service requirement on server core installations. - V-57457 - Clarified requirement for location of Windows Error Reporting data. - V-57461 - Removed Windows Error Reporting port requirement, not security related. - V-57655 - Clarified requirement based on GPOS SRG update. **Windows 2012 and 2012 R2 DC Benchmark, V2R6:** - V-32272, V-32274, and V-40237 - Updated OVAL to reference current certificates.	
V2R5	- Windows 2012/2012 R2 DC STIG, V2R4	- V-1107 - Changed password history to "24", consistent with other Windows STIGs. - V-1112 - Clarified Check, replaced DumpSec with PowerShell query. - V-26473 - Clarified requirement, retargeted current Rule to domain controllers (separate Rule added for member servers). - V-26602 - Corrected FTP service name. - V-36680 - Corrected location to determine if Windows Store has been installed. - V-57637 - Changed to CAT II. Updated PowerShell query used to determine AppLocker effective policy. - V-57721 - Corrected typo in location of event viewer file. **Windows 2012 and 2012 R2 DC Benchmark, V2R5:** - Added SCAP 1.2 Validation Fixes to Windows 2012 DC STIG.	22 July 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1107 - Modified the OVAL content to match the manual STIG update. - V-26473 - Split rules for DC/MS. - V-36680 - Corrected path referenced to determine if Windows Store has been installed.	
V2R4	- Windows 2012/2012 R2 DC STIG, V2R3	- Added Section 1.7 Product Approval Disclaimer to the STIG Overview document. - V-1080 and V-1088 - Removed requirement due to excessive event generation. - V-1131 - Removed requirement referencing Enpasflt password filter, which is no longer supported. - V-1150 - Raised requirement for Windows built-in password complexity to a CAT II. - V-1152 - Clarified requirement to maintain the default permissions. - V-14783 - Removed references to SAMI data. - V-15488 - Updated Check to use PowerShell to identify accounts that do not require smart cards. Clarified that requirement includes administrator accounts. - V-15671 - Removed requirement preventing root certificate updates from Microsoft. - V-26070 - Clarified requirement to maintain the default permissions. - V-26544 and V-26545 - Removed requirement due to excessive event generation. - V-26579 - Corrected event log size policy name in Fix. - V-26580, V-26581 - Corrected event log size policy name in Fix. - V-26582 - Corrected event log size policy name in Fix. - V-32282 - Clarified requirement to maintain the default permissions. - V-36669 - Removed requirement due to excessive event generation. - V-36690, V-36691 - Removed non-security-related requirement.	22 April 2016

	REVISION HISTORY		
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-40166 - Removed requirement for SAMI audit data archive. **Windows 2012 and 2012 R2 DC Benchmark, V2R4:** - V-3469 - Modified OVAL to produce a passing result when the value equals 0. - V-7002, V-8316 - Added OVAL. - V-15671, V-26544, V-26545, V-36669, V-36690, and V-36691 - Disabled Rule.	
V2R3	- Windows 2012/2012 R2 DC STIG, V2R2	- V-1074 - Removed Symantec from requirement. - V-14254 - Removed, retargeted to member servers only. - V-36663, V-36664, and V-40195 - Clarification for virtual machines. - V-57637 - Application Whitelisting requirement was raised to CAT I. - V-57657 - Removed requirement. - The following were updated to correct policy names as wells as miscellaneous text updates: V-1141, V-1158, V-1174, V-4116, V-4438, V-21956, V-21964, and V-57639. - Removed EMET requirements: V-36701, V-36702, V-36703, V-36704, V-36705, V-36706, and V-39137. **Windows 2012 and 2012 R2 DC Benchmark, V2R3:** - V-15823 - Matched file extensions case insensitivity. - V-36701, V-36702, V-36703, V-36704, V-36705, V-36706, and V-39137 - Removed requirement. - V-40237 - Updated to search both path locations. - V-57633, V-57635, V-57639, and 57721 - Configured new OVAL. - Removed unreferenced OVAL content.	23 October 2015
V2R2	- Windows 2012/2012	- V-1090 and V-15719 - Requirement is NA for non-domain joined systems.	24 July 2015

14

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	R2 DC STIG, V2R1	- V-15680 - Requirement is NA for domain joined systems, retargeted to member servers only. - V-21954 - Update Check procedure to verify bits, not direct registry value. - V-26482 - Updated to allow for "Virtual Machines" when Hyper-V role is installed. - V-57637 - Note added on future Severity upgrade. - EMET - The following requirements are applicable to unclassified systems: - V-39137 - Updated to require EMET v5.x. Support for v4.x ended 09 June 2015. - V-36701, V-36702, V-36703, V-36704, V-36705, and V-36706. **Windows 2012 and 2012 R2 DC Benchmark, V2R2:** - V-1090 - Added applicability statement. - V-1099 - Modified check for account lockout policy. - V-3339, V-3340, V-4443, and V-4445 - Modified check against registry value. - V-15680 - Added applicability statement. Setting is NA for domain systems. - V-15719 - Added applicability statement. - V-21954 - Updated registry check. - V-26482 - Added Hyper-V check. - V-32272 - Added registry check. - V-32274 - Added registry check. - V-39137 - Updated check for EMET.	