MICROSOFT WINDOWS SERVER 2016 STIG REVISION HISTORY

Version 2, Release 5

14 November 2022

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R5	- Windows Server 2016 STIG, V2R4	- WN16-00-000030, WN16-00-000070, WN16-00-000100, WN16-00-000210, WN16-00-000220, WN16-00-000330, WN16-00-000340, WN16-CC-000090, WN16-CC-000110, WN16-MS-000020, WN16-MS-000030, WN16-MS-000040, WN16-MS-000050, WN16-MS-000120, WN16-MS-000310, WN16-MS-000340, WN16-MS-000370, WN16-MS-000380, WN16-MS-000400, WN16-MS-000410, WN16-MS-000420 - Changed wording in the Check text from “standalone” to “standalone or nondomain-joined”. - WN16-00-000230 - Changed wording in the Check and Fix text from “standalone” to “standalone or nondomain-joined”. - WN16-00-000240 - Updated Check text: “A properly configured McAfee Application Control and Change Control (MACC) module will meet the requirement for file integrity checking.” - WN16-00-000450 - Changed wording in the Check text from “standalone” to “standalone or nondomain-joined” and updated hyperlinks in Check and Fix text. - WN16-AU-000020 - Changed wording in the Rule Title, Check, and Fix text from “standalone” to “standalone or nondomain-joined”. - WN16-DC-000140 – Corrected punctuation in Rule Title. - WN16-MS-000010 - Changed wording in the Rule Title and Check text from “standalone” to “standalone or nondomain-joined”. WN16-SO-000380 - Changed wording in the Discussion from “standalone” to “standalone or nondomain-joined”. - Some Rule IDs and CCIs updated due to minor changes in content management system.	14 November 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R4	- Windows Server 2016 STIG, V2R3	- WN16-00-000220 - Updated Fix text: Configure all enabled “user” accounts to require passwords. - WN16-MS-000390 - Removed from Check text: “and standalone systems”. - WN16-PK-000010, WN16-PK-000020 - Removed all deprecated DoD Root CA 2 references.	31 May 2022
V2R3	- Windows Server 2016 STIG, V2R2	- WN16-00-000030 - Updated Discussion/Fix to highly recommend use of LAPS, and AO can approve other solutions. - WN16-00-000140, WN16-00-000240, WN16-00-000320 - Replaced HBSS references with ESS. - WN16-00-000190 - Updated Check/Fix for HKEY_LOCAL_MACHINE\SYSTEM to include Server Operators – Read – This Key and subkeys (domain controllers only). - WN16-00-000240 - Removed reference to Policy Auditor. - WN16-00-000290 - Revised last six digits of Rule ID SV number; no other change. - WN16-CC-000110 - Removed Check text wording: “Current hardware and virtual environments may not support virtualization-based security features, including Credential Guard, due to specific supporting requirements, including a TPM, UEFI with Secure Boot, and the capability to run the Hyper-V feature within a virtual machine.”	01 November 2021
V2R2	- Windows Server 2016 STIG, V2R1	- WN16-00-000320 - Removed HBSS wording. Updated Check and Fix and added Note section. - WN16-00-000470, WN16-00-000480 - Corrected grammar in Check finding statement. - WN16-CC-000421 - Replaced group title with SRG-OS-000095-GPOS-00049. - WN16-DC-000080 - Removed the File Explorer option from the Check. This option	04 May 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		could impact SYS volume properties and cause corruption.	
V2R1	- Windows Server 2016 STIG, V1R12	- 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 V1R12 to V2R1. - WN16-00-000120 - Added language and PowerShell checks that AV exists on the server. Option given for Windows Defender or approved third-party solution. - WN16-00-000240 - 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.” - WN16-MS-000120 - Added Severity Override Guidance. - WN16-PK-000010 - Removed “If an expired certificate (“Valid to” date)” wording. - WN16-PK-000020, WN16-PK-000030 - Removed “If an expired certificate (“Valid to” date)” wording. Updated identified certificates.	13 November 2020
V1R12	- Windows Server 2016 STIG, V1R11	- V-102623 - In Check text, separated registry settings. In Fix text, added >> Explorer Frame Pane.	17 June 2020
V1R11	- Windows Server 2016 STIG, V1R10	- V-73259 - Added Group Title. Updated Check Text to add built-in default account (Renamed, Disabled, SID ending in 503). - V-102623 - Added requirement: The Windows Explorer Preview pane must be disabled for Windows Server 2016.	15 May 2020
V1R10	- Windows Server 2016 STIG, V1R9	- V-91779 – Revised Discussion to reflect that 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	24 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		lifetime, and changing again reduces the risk of issues."	
V1R9	- Windows Server 2016 STIG, V1R8	- V-73237 - Upgraded Severity Level for requirement to CAT II in line with the Windows Server 2019 STIG. - V-73261 - Updated requirement with note excluding Trust Domain Objects (TDOs). - V-73271 - Added note to requirement regarding Adobe Preflight certificate files. - V-73281 - Modified Check and Fix text to require "DoD approved HBSS software". - V-73497 - Corrected typo in the Discussion replacing Windows 10 with Windows Server 2016. - V-73513 - Upgraded Severity Level for requirement to CAT II in line with the Windows Server 2019 STIG. - V-73515 - Upgraded Severity Level for requirement to CAT I in line with the Windows Server 2019 STIG. - V-73517 - Removed Virtualization-based Protection of Code Integrity requirement. - V-73559 - Updated requirement with applicability note for unclassified systems. - V-73731 - Updated Check Text with correct user right. - V-90355 - Added Rule Title to requirement. Corrected typo in the Discussion replacing Windows 10 with Windows Server 2016. - V-90357 - Corrected typo in the Discussion replacing Windows 10 with Windows Server 2016.	26 July 2019
V1R8	- Windows Server 2016 STIG, V1R7	- V-73607 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Added new certificate. Removed expired certificates. - V-73609 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Removed expired certificate.	26 April 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Updated the following requirements to include command line instructions for server core installations: - V-73309, V-73311, V-73313, V-73315, V-73317, V-73319, V-73321, V-73323, V-73325, V-73809, V-73623, V-73625, V-73729, V-73731, V-73733, V-73735, V-73737, V-73739, V-73741, V-73743, V-73745, V-73747, V-73749, V-73751, V-73753, V-73755, V-73757, V-73759, V-73761, V-73763, V-73765, V-73767, V-73769, V-73771, V-73773, V-73775, V-73777, V-73779, V-73781, V-73783, V-73785, V-73787, V-73789, V-73791, V-73793, V-73795, V-73799, V-73801, V-73803.	
V1R7	- Windows Server 2016 STIG, V1R6	- V-91779 - Added KRBTGT password reset requirement. - V-73515 - Updated to allow only Enabled with UEFI Lock. Changed STIG ID to "MS". - V-73659 - Removed by DoD Consensus group, does not mitigate contemporary threats. - V-73665 - Added command for server core installations. - V-73671 - Removed by DoD Consensus group due to functional issues caused. - V-73685 - Added Note about potential trust issue when RC4 is still enabled in domains. - V-73689 and V-73703 - Removed by DoD Consensus group due to limited value. - V-73723 and V-73725 - Removed by DoD Consensus group, addressed by machine inactivity setting. - V-78127 - Added command for server core installations. - V-90355 - Added Secure Boot requirement. - V-90357 - Added UEFI requirement.	08 February 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-90359 - Added Other Object Access success audit requirement. - V-90361 - Added Other Object Access failure audit requirement.	
V1R6	- Windows Server 2016 STIG, V1R5	- V-73443, V-73445, V-73477, and V-73479 - Corrected group policy path. - V-73221, V-73733, V-73759, V-73771, and V-73775 - Removed exception note referencing AD admin platforms. - V-73269 - Removed requirement, addressed by product STIG. - V-73645 - Updated to clarify "0" is not allowed. - V-73515 - Updated to note as NA for domain controllers. Updated link to Microsoft documentation.	26 October 2018
V1R5	- Windows Server 2016 STIG, V1R4	- V-73235 - Corrected typo in reference to NSA document, updated link. - V-73605, V-73607, and V-7609 - Updated with additional certificate. Added certificate expiration dates for reference. - V-73677 - Updated to NA for domain controllers, changed STIG ID. **Windows Server 2016 Benchmark, V1R6:** - V-73369 - Updated to check all files in the log path, DSA Working Directory, and DSA Database file directory. - V-73405 - Updated Application event log permissions check to address issue with Java-based scan engines. - V-73407 - Updated Security event log permissions check to address issue with Java-based scan engines. - V-73409 - Updated System event log permissions check to address issue with Java-based scan engines. - V-73605 - Updated DoD Root CA OVAL content to include additional certificate. - V-73609 - Updated DoD CCEB Interoperability Root CA OVAL content to include additional certificate.	27 July 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-73645 - Updated Machine Inactivity OVAL content to include a value of "0" will result in a finding. - V-73677 - Updated to NA for domain controllers.	
V1R4	- Windows Server 2016 STIG, V1R3	- V-73233 - Updated allowed exceptions note. - V-73243 - Removed antivirus signature requirement, addressed by AV product STIGs. - V-73389 - Updated group policy object auditing method and scope. - V-73421 - Removed Other Account Management failure event audit requirement as NA. - V-73425 - Removed Security Group Management failure event audit requirement as NA. - V-73485 - Removed Security System Extension failure event audit requirement as NA. **Windows Server 2016 Benchmark, V1R5:** - Updated CPE OVAL to pass only for Windows Server 2016. - V-73421, V-73425, and V-73485 - Disabled OVAL due to STIG rule removal.	27 April 2018
V1R3	- Windows Server 2016 STIG, V1R2	- The SecGuide custom admin template files have been updated to include additional configuration settings. - V-73241 - Removed specific antivirus product referenced. - V-73259 - Corrected note referring to built-in administrator as disabled instead of renamed. - V-73299 - Updated to allow alternate method for disabling SMBv1. - V-73375 - Clarified changes from schema update to support Exchange are not a finding. - V-73535 - Removed requirement for untrusted font blocking due to issues.	26 January 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-73605 - Clarified details apply to unclassified systems, refers to PKE documentation for other systems. - V-73615 - Clarified various formats may exist for individual identifiers. - V-73647 - Removed short version of banner text as NA. - V-78123 - Added as alternate method for disabling SMBv1 server. - V-78125 - Added as alternate method for disabling SMBv1 client. - V-78127 - Added requirement for unresolved SIDs found on user rights. - Corrected STIG ID referenced in Check for the following: V-73431, V-73443, V-73445, V-73447, V-73477, and V-73479. **Windows Server 2016 Benchmark, V1R4:** - Updated platform-specification for applicability determinations. - V-73299 - Added new OVAL content for the SMBv1 Protocol requirement. - V-73405, V-73407, V-73409, and V-73535 - New OVAL development for Windows Server 2016. - V-78123 - Added new OVAL content for the SMBv1 Server requirement. - V-78125 - Added new OVAL content for the SMBv1 Client requirement.	
V1R2	- Windows Server 2016 STIG, V1R1	- V-73223 and V-73231 - Corrected typo in command used to verify requirement on member servers. - V-73261 and V-73263 - Updated member server query to filter for local accounts only. - V-73309 - Updated account lockout duration to 15 minutes or greater.	28 July 2017
V1R1	- N/A	- Initial Release.	20 January 2017