MICROSOFT WINDOWS SERVER 2019 STIG REVISION HISTORY

Version 2, Release 8

09 November 2023

Developed by DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R8	- Windows Server 2019 STIG, V2R7	- WN19-00-000020 - Updated check text to include settings; revised fix text. - WN19-00-000440 - Updated fix with new web link. - WN19-CC-000250 - Updated wording in fix to remove “and Preview Builds”. - WN19-CC-000530 - Added PowerShell Transcription requirement. - WN19-DC-000320, WN19-SO-000060, WN19-SO-000070, WN19-SO-000080, WN19-SO-000110, WN19-SO-000160, WN19-SO-000170, WN19-SO-000190, WN19-SO-000200 - Rule IDs updated due to changes in content management system. - WN19-PK-000010 - Updated certificate type DoD CA 6.	09 November 2023
V2R7	- Windows Server 2019 STIG, V2R6	- WN19-00-000020 - Updated vulnerability discussion and fix text. - WN19-AU-000020 - Corrected misspelling in Fix.	07 June 2023
V2R6	- Windows Server 2019 STIG, V2R5	- WN19-00-000080 - In Check, removed wording: “This is applicable to unclassified systems. For other systems, this is NA.” In Check and Fix, revised link for AppLocker Deployment Guide. Replaced “whitelist” with “allowlist” throughout requirement. - WN19-00-000220 - Revised Check text and removed ESS (MACC). - WN19-AU-000150 - Removed requirement to audit Logon/Logoff - Account Lockout successes. - WN19-DC-000270 - Removed requirement to audit DS Access - Directory Service Changes failures. - WN19-MS-000100 - Removed wording “on non-domain-joined systems” from Check. - WN19-PK-000010 - Revised Fix to add PKI link for DOD certificates. - WN19-PK-000030 - Revised Check and Fix to reflect updated certificates and added PKI link for DOD certificates to Fix.	11 May 2023

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- WN19-SO-000140 - Revised the requirement referenced in the Check and Fix to WN19-SO-000130. - Some Rule IDs updated due to changes in content management system.	
V2R5	- Windows Server 2019 STIG, V2R4	- WN19-00-000020, WN19-00-000060, WN19-00-000090, WN19-00-000190, WN19-00-000200, WN19-00-000300, WN19-00-000310, WN19-CC-000080, WN19-CC-000110, WN19-MS-000020, WN19-MS-000030,WN19-MS-000050, WN19-MS-000080, WN19-MS-000090, WN19-MS-000110, WN19-MS-000120, WN19-MS-000140 - Changed wording in the Check text from “standalone” to “standalone or nondomain-joined”. - WN19-00-000210 - Changed wording in the Check and Fix text from “standalone” to “standalone or nondomain-joined”. - WN19-00-000220 - Updated Check text: “A properly configured McAfee Application Control and Change Control (MACC) module will meet the requirement for file integrity checking.” - WN19-00-000440 - Changed wording in the Check text from “standalone” to “standalone or nondomain-joined” and revised link in Fix text. - WN19-AU-000020 - Changed wording in the Rule Title, Check, and Fix text from “standalone” to “standalone or nondomain-joined”. - WN19-DC-000430 - Changed script link in the Fix text. - WN19-MS-000010, WN19-MS-000040, WN19-MS-000060, WN19-MS-000070, WN19-MS-000130 - Changed wording in the Rule Title and Check text from “standalone” to “standalone or nondomain-joined”. - WN19-PK-000020 - Changed Check text for Issuer: CN=DoD Interoperability Root CA 1 to CA 2.	14 November 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- WN19-SO-000310 - Changed wording in Rule Title from “standalone” to “standalone or nondomain-joined”. - Some Rule IDs and CCIs updated due to minor changes in content management system.	
V2R4	- Windows Server 2019 STIG, V2R3	- WN19-00-000380 - Updated the rule title: Windows Server 2019 must not “have” the Server Message Block (SMB) v1 protocol installed. - WN19-CC-000110 - Removed device guard wording and replaced with virtualization-based security in Check text. - WN19-MS-000100 - Removed from Check text: “and standalone systems”. - WN19-PK-000010, WN19-PK-000020 - Removed all deprecated DOD Root CA 2 references.	31 May 2022
V2R3	- Windows Server 2019 STIG, V2R2	- WN19-00-000020 - Updated Check/Fix to highly recommend use of LAPS, and AO can approve other solutions. - WN19-00-000120, WN19-00-000220, WN19-00-000290 - Replaced HBSS references with ESS. - WN19-00-000170 - Updated registry permissions to include Server Operators – Read – This Key and subkeys (Domain controllers only). - WN19-00-000260 - Revised last six digits of Rule ID SV number; no other change. - WN19-EP-000010, WN19-EP-000020, WN19-EP-000030, WN19-EP-000040, WN19-EP-000050, WN19-EP-000060, WN19-EP-000070, WN19-EP-000080, WN19-EP-000090, WN19-EP-000100, WN19-EP-000110, WN19-EP-000120, WN19-EP-000130, WN19-EP-000140, WN19-EP-000150, WN19-EP-000160, WN19-EP-000170, WN19-EP-000180, WN19-EP-000190, WN19-EP-000200, WN19-EP-000210, WN19-EP-000220, WN19-EP-000230, WN19-EP-000240, WN19-EP-000250, WN19-EP-000260,	01 November 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		WN19-EP-000270, WN19-EP-000280, WN19-EP-000290 - Removed Exploit Protection requirements. Settings for EMET deprecated by Microsoft. - WN19-MS-000140 - 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."	
V2R2	- Windows Server 2019 STIG, V2R1	- WN19-00-000290 - Removed HBSS wording. Updated Check and Fix and added Note section. - WN19-CC-000451 - Replaced group title with SRG-OS-000095-GPOS-00049. - WN19-DC-000080 - Removed the File Explorer option from the Check. This option could impact SYS volume properties and cause corruption.	04 May 2021
V2R1	- Windows Server 2019 STIG, V1R5	- 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 V1R5 to V2R1. - WN19-00-000110 - Added language and PowerShell checks that AV exists on the server. Provided option for Windows Defender or approved third-party solution. - WN19-00-000220 - 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." - WN19-MS-000140 - Added Severity Override Guidance. - WN19-PK-000010 - Removed "If an expired certificate ("Valid to" date)" wording. - WN19-PK-000020, WN19-PK-000030 - Removed "If an expired certificate ("Valid	13 November 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		to" date)" wording. Updated identified certificates.	
V1R5	- Windows Server 2019 STIG, V1R4	- V-102625 - In Check text, separated registry settings. In Fix text, added >> Explorer Frame Pane.	17 June 2020
V1R4	- Windows Server 2019 STIG, V1R3	- V-93175 - Updated registry path spacing. - V-102625 - Added requirement: The Windows Explorer Preview pane must be disabled for Windows Server 2019.	15 May 2020
V1R3	- Windows Server 2019 STIG, V1R2	- V-93211 – 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 lifetime, and changing again reduces the risk of issues."	24 January 2020
V1R2	- Windows Server 2019 STIG, V1R1	- V-93221 - Added note to requirement regarding Adobe Preflight certificate files. - V-93411 - Updated requirement with applicability note for unclassified systems. - V-93247 - Removed Virtualization-based Protection of Code Integrity requirement. - V-93439 - Updated requirement with note excluding Trust Domain Objects (TDOs).	26 July 2019
V1R1	- NA	- Initial Release.	05 June 2019