MICROSOFT (MS) DEFENDER ANTIVIRUS STIG REVISION HISTORY

Version 2, Release 4

31 May 2022

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R4	- Microsoft Windows Defender AV STIG, V2R3	- STIG title: Revised from Microsoft Windows Defender Antivirus to Microsoft Defender Antivirus. - All requirements: In all Check text, revised configuration path reference to Microsoft Defender. Revised text as needed for grammar/punctuation.	31 May 2022
V2R3	- Microsoft Windows Defender AV STIG, V2R2	- In Overview Section 2.2, removed Windows 2012 and 8.1 references. - WNDF-AV-000030 - Revised registry path: HKLM\Software\Policies\Microsoft\Windows Defender\Signature Updates.	01 November 2021
V2R2	- Microsoft Windows Defender AV STIG, V2R1	- In Overview Section 3, Applicability and Usage, revised wording and removed conflicting guidance. - WNDF-AV-000004 - Removed 2016/2019 references because operating systems were updated 15 November 2019 with AV guidance.	04 May 2021
V2R1	- Microsoft Windows Defender AV STIG, V1R9	- 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 V1R9 to V2R1. - WNDF-AV-000005 - Added exception language into rule to allow file/folders to be excluded from scanning. - WNDF-AV-000028 - Modified check text to "third-party anti-spyware".	13 November 2020
V1R9	- Microsoft Windows Defender AV STIG, V1R8	- V-75241 - Updated Check to include NA statement if third-party spyware is installed. - V-75243 - Updated Check to include NA statement if third-party antivirus protection is installed.	15 May 2020
V1R8	- Microsoft Windows Defender AV STIG, V1R7	- V-75147 - Revised requirement to configure Windows Defender AV to block Potentially Unwanted Application feature.	24 April 2020
V1R7	- Microsoft Windows	- V-75153 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs.	24 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	Defender AV STIG, V1R6 - Microsoft Windows Defender AV Overview	- V-75167 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs. - Modified Overview to include Windows Server 2019 as being subject to the Windows Defender STIG inspection.	
V1R6	- Microsoft Windows Defender AV STIG, V1R5	- V-75167 - Corrected back to properties for "Enabled" as the conflicting STIG ID in the Windows OS STIG has been removed.	26 July 2019
V1R5	- Microsoft Windows Defender AV STIG, V1R4	- V-75167 - Clarified requirement as it relates to the Windows Operating System and McAfee STIGS. - V-75153 - Added check and fix verbiage for both Win10 and Server 2016 versions.	26 April 2019
V1R4	- Microsoft Windows Defender AV STIG, V1R3	- Updated Overview document to add Applicability and Usage section. - V-75153 - Removed the allowance of the value “Disabled”. - V-75247 - Separated out each threat level. Modified this requirement for threat level Severe. - V-79965 - Added requirement for threat level High. - V-79967 - Added requirement for threat level Medium. - V-79971 - Added requirement for threat level Low.	27 April 2018
V1R3	- Microsoft Windows Defender AV STIG, V1R2	- V-75207 – Updated Fix Text.	26 January 2018
V1R2	- Microsoft Windows Defender AV STIG, V1R1	- V-75161 – Added NA statement for unclassified systems. - V-75163 – Added NA statement for unclassified systems. - V-75167 – Added NA statement for unclassified systems. - V-75207 – Added NA statement for unclassified systems. - V-75147 – Updated to add custom admin	31 October 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		template information. - V-77965 – Added new requirement to block executable content from email client and webmail. - V-77967 – Added new requirement to block Office applications from creating child processes. - V-77969 – Added new requirement to block Office applications from creating executable content. - V-77971 – Added new requirement to block Office applications from injecting into other processes. - V-77973 – Added new requirement to impede JavaScript and VBScript to launch executables. - V-77975 – Added new requirement to block execution of potentially obfuscated scripts. - V-77977 – Added new requirement to block Win32 imports from macro code in Office. - V-77979 – Added new requirement to prevent user and apps from accessing dangerous websites.	
V1R1	- N/A	- Initial Release.	26 July 2017