WINDOWS 2012/2012 R2
MEMBER SERVER (MS) STIG
REVISION HISTORY

Version 2, Release 11

26 January 2018

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R11	- Windows 2012/2012 R2 MS STIG	- V-6840 - Updated to use Windows queries instead of DumpSec application. - 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 - Removed requirement Audit Computer Account Management Success, applies 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. - V-78063 - Added Audit Other System Events Failures to align with Windows 2016 STIG. **Windows 2012 and 2012 R2 MS Benchmark, V2R11:** - V-26531 - Removed OVAL content, requirement removed from the manual STIG. - V-26532 - Removed OVAL content, requirement removed from the manual STIG. - V-26554 - Removed OVAL content, requirement removed from the manual STIG.	26 January 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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 MS STIG	- 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-32272 - Clarified details apply to unclassified systems, refers to PKE documentation for other systems. - V-43239 - Changed requirement to enable command line data to be included in process creation events. - 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 SMBv1 is found. Updated Fix to use custom administrative template for configuration. - V-73805 - Updated to allow alternate method for disabling SMBv1. - V-75915 - Added requirement for unresolved SIDs found on user rights.	27 October 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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 MS Benchmark, V2R10:** - Removed OVAL content for the following as requirement has been removed from the STIG: V-26475, V-26477, 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 SMBv1 Server requirement to pass on Windows Server 2012 R2. - V-73523 - Updated the OVAL content for SMBv1 Client requirement to pass on Windows Server 2012 R2. Updated DependOnService to be a finding only if SMBv1 is found and not specifically for other defaults. - V-73805 - Updated the OVAL content for SMBv1 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.	
V2R9	- Windows 2012/2012 R2 MS STIG	- 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 - Updated Check to more accurately verify FTP configuration. - V-1121 - Updated Check to more accurately verify FTP configuration. - V-14243 - Updated Rule Title to more accurately reflect requirement.	28 July 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26602 - Clarified Rule Title; service must be disabled unless required. - V-36439 - Updated Fix to use custom admin template instead of direct registry update. - V-36451 - Clarified requirement; policy required, technical means to enforce. **Windows 2012 and 2012 R2 MS 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.	
V2R8	- Windows 2012/2012 R2 MS STIG	- V-1074 - Updated requirement consistent with other Windows STIGs. Changed STIG ID. - V-1152 - Clarified permissions must be at least as restrictive as defaults. - V-15505 - Clarified versions of service being verified. - V-26070 - Clarified permissions must be at least as restrictive as defaults. - 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 - Added requirement to disable Server Message Block (SMB) v1 on the Windows 2012 SMB server. - V-73523 - Added requirement to disable Server Message Block (SMB) v1 on the Windows 2012 SMB client. - V-73805 - Added requirement to disable Server Message Block (SMB) v1 on Windows 2012 R2. **Windows 2012 and 2012 R2 MS Benchmark, V2R8:**	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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 SMBv1 protocol for the SMB server is disabled for Windows 2012. - V-73523 - Added OVAL to check if the SMBv1 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 MS STIG	- V-26496 - Updated to include application exception. - V-32274 - Updated expired certificate with replacement. - V-72753 - Added requirement to disable WDigest. - 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, V-57479. - The following were removed by DoD Consensus: V-1158, V-1159, V-3457, V-3458, V-4446, V-14254, V-15719, V-16005, V-26471, V-26491, V-26495, V-36772. **Windows 2012 and 2012 R2 MS Benchmark, V2R7:** - 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-14254, 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, V-57479.	27 January 2017
V2R6	- Windows 2012/2012	- V-1155 - Updated to allow "Local account and member of Administrators group".	28 October 2016

UNCLASSIFIED

Windows 2012/2012 R2 MS STIG Revision History, V2R11
26 January 2018

DISA
Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	R2 MS STIG	- V-1163 - Removed data in False Positive field, duplicated in Check. - V-1164 - Removed data in False Positive field, duplicated in Check. - V-15505 - Updated for v5 of McAfee agent. - V-32272 - Updated PKE related requirement with current certificates. - 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 - Removed BIOS related requirement as outside of OS scope. - V-36664 - Removed BIOS related requirement as outside of OS scope. - V-36667 - Clarified for virtual machines and systems with network attached storage. - V-36668 - Clarified for virtual machines and systems with network attached storage. - 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 MS Benchmark, V2R6:** - V-1155 - Updated to allow "Local account and member of Administrators group". - V-32272 - Updated OVAL to reference current certificates.	

6

UNCLASSIFIED

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-32274 - Updated OVAL to reference current certificates. - V-40237 - Updated OVAL to reference current certificates.	
V2R5	- Windows 2012/2012 R2 MS STIG	- V-1107 - Changed password history to "24", consistent with other Windows STIGs. - V-1112 - Clarified Check, replaced DumpSec with PowerShell query. - V-1155 - Updated to require use of "Local account" to deny access on member servers. - V-26473 - Clarified requirement, added separate Rule for member servers. - V-26486 - Updated to require use of "Local account" to deny access on member servers. - V-26602 - Corrected FTP service name. - V-36680 - Corrected location to determine if Windows Store has been installed. - V-45589 - Removed requirement to define a group for local administrator accounts. - 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 MS Benchmark, V2R5:** - Added SCAP 1.2 Validation Fixes to Windows 2012 MS STIG. - V-1107 - Modified the OVAL content to match the manual STIG update. - V-1155 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-26473 - Split rules for DC/MS, clarification of MS allowed exceptions. - V-26486 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-36680 - Corrected path referenced to determine if Windows Store has been installed. - V-45589 - Disabled rule in OVAL.	22 July 2016
V2R4	- Windows 2012/2012	- Added Section 1.7 Product Approval Disclaimer to the STIG Overview document.	22 April 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	R2 MS STIG	- V-1080 - Removed requirement due to excessive event generation. - 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-15671 - Removed requirement preventing root certificate updates from Microsoft. - V-26070 - Clarified requirement to maintain the default permissions. - V-26544 - Removed requirement due to excessive event generation. - V-26545 - Removed requirement due to excessive event generation. - V-26579 - Corrected event log size policy name in Fix. - V-26580 - Corrected event log size policy name in Fix. - 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 - Removed non-security-related requirement. - V-36691 - Removed non-security-related requirement. - V-40166 - Removed requirement for SAMI audit data archive. **Windows 2012 and 2012 R2 MS Benchmark, V2R4:** - V-1155 - Modified the OVAL to include a check for the Local account and Local account and member	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		of Administrators, which includes the NT Authority prefix. Modified the OVAL to include an equals check for the Enterprise Admins group. - V-7002 - Added OVAL. - V-15671 - Disabled Rule. - V-26483 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26484 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26485 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26486 - Modified the OVAL to include a check for the Local account and Local account and member of Administrators, which includes the NT Authority prefix. Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26544 - Disabled Rule. - V-26545 - Disabled Rule. - V-36669 - Disabled Rule. - V-36690 - Disabled Rule. - V-36691 - Disabled Rule. - V-57721 - Added OVAL.	
V2R3	- Windows 2012/2012 R2 MS STIG	- V-1074 - Removed Symantec from requirement. - V-14254 - Retargeted to member servers only. - V-36663 - Clarification for virtual machines. - V-36664 - Clarification for virtual machines. - 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, V-57639. - Removed EMET requirements: V-36701, V-36702, V-36703, V-36704, V-36705, V-36706, V-39137. **Windows 2012 and 2012 R2 MS Benchmark, V2R3:** - V-14254 Removed from benchmark to coincide with removal from the manual STIG. - V-15823 Matched file extensions case insensitivity.	23 October 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-36701 Removed requirement. - V-36702 Removed requirement. - V-36703 Removed requirement. - V-36704 Removed requirement. - V-36705 Removed requirement. - V-36706 Removed requirement. - V-39137 Removed requirement. - V-40237 Updated to search both path locations. - V-57633 Configured new OVAL. - V-57635 Configured new OVAL. - V-57639 Configured new OVAL. - V-57721 Configured new OVAL. - Removed unreferenced OVAL content.	
V2R2	- Windows 2012/2012 R2 MS STIG	- V-1090 - Requirement is NA for non domain joined systems. - V-15680 - Requirement is NA for domain joined systems, retargeted to member servers only. - V-15719 - Requirement is NA for non domain joined systems. - 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, V-36706. **Windows 2012 and 2012 R2 MS Benchmark, V2R2:** - V-1090 Added applicability statement. - V-1099 Modified check for account lockout policy. - V-3338 Modified check against registry value. - V-3339 Modified check against registry value. - V-3340 Modified check against registry value. - V-4443 Modified check against registry value. - V-4445 Modified check against registry value. - V-15680 Added applicability statement. Setting is NA for domain systems.	24 July 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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.	