

UNCLASSIFIED



WINDOWS SERVER 2008 MEMBER SERVER STIG REVISION HISTORY

Version 6, Release 39

26 January 2018

Developed by DISA for the DoD

UNCLASSIFIED

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V6R39	- Windows 2008 MS STIG	- V-15823 - Clarified noted exceptions.	26 January 2018
V6R38	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-1074 - Removed specific antivirus product referenced. - V-1089 - Removed short version of banner text as NA. - V-32272 - Clarified that details apply to unclassified systems; refers to PKE documentation for other systems. - V-73523 - Modified Check to only be a finding if SMBv1 is found. - V-75915 - Added requirement for unresolved SIDs found on user rights. <p>Windows 2008 MS Benchmark, V6R40:</p> <ul style="list-style-type: none"> - V-32282 - Added OVAL content to the benchmark. - V-73523 - Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults. 	27 October 2017
V6R37	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-1098 - Updated reset account lockout counter to 15 minutes or greater. - V-1099 - Updated account lockout duration to 15 minutes or greater. - 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. - V-26602 - Clarified Rule Title, service must be disabled unless required. - V-3337 - Removed exception note, no longer applicable. - V-36451 - Clarified requirement - policy required, technical means to enforce. <p>Windows 2008 MS Benchmark, V6R39:</p>	28 July 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - 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. 	
V6R36	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-1074 - Moved antivirus signature to separate requirement (V-40175). 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 - Moved antivirus signature to separate requirement (previously part of V-1074). Updated to require configuration of daily checks as well as a maximum age of one week. - V-73519 - Added requirement to disable Server Message Block (SMB) v1 on the SMB server. - V-73523 - Added requirement to disable Server Message Block (SMB) v1 on the SMB client. <p>Windows 2008 MS Benchmark, V6R38:</p> <ul style="list-style-type: none"> - 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. - V-73523 - Added OVAL to check if the SMBv1 protocol for the SMB client is disabled. 	28 April 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V6R35	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-32274 - Updated expired certificate with replacement. - V-14262 - Removed requirement to disable IPv6. - Removed Error Reporting requirements: V-15714, V-15715, V-15717, V-56511, 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-14254, V-15719, V-16005. - V-1103 - Removed the following user rights at DoD Consensus request: <ul style="list-style-type: none"> - Adjust memory quotas for a process - Increase a process working set - Log on as a batch <p>Windows 2008 MS Benchmark, V6R37:</p> <ul style="list-style-type: none"> - V-1103 - Updated OVAL content in conjunction with modifications to the requirement in the manual STIG. - 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-14262, V-15714, V-15715, V-15717, V-15719, V-16005, V-56511, 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
V6R34	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - 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-36663 - Removed BIOS related requirement as outside of OS scope. 	28 October 2016

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-36664 - Removed BIOS related requirement as outside of OS scope. - 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. <p>Windows 2008 MS Benchmark, V6R36:</p> <ul style="list-style-type: none"> - V-26604 - Added new OVAL content. - V-26605 - Added new OVAL content. - V-26606 - Added new OVAL content. - V-32272 - Updated OVAL to reference current certificates. - V-32274 - Updated OVAL to reference current certificates. - V-40237 - Updated OVAL to reference current certificates. 	
V6R33	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-1107 - Clarified with regard to selection of 24 for password history. - V-1112 - Clarified Check, removed Windows 2003 references. - V-16006 - Removed general requirement, replaced with specific service requirements. - V-26600 - Replaced V-16006 with specific service requirement. - V-26602 - Replaced V-16006 with specific service requirement. - V-26604 - Replaced V-16006 with specific service requirement. - V-26605 - Replaced V-16006 with specific service requirement. - V-26606 - Replaced V-16006 with specific service requirement. 	22 July 2016

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		Windows 2008 MS Benchmark, V6R35: - Added SCAP 1.2 Validation Fixes to Windows 2008 MS STIG. - V-26600 - Added new OVAL content. - V-26602 - Added new OVAL content.	
V6R32	- Windows 2008 MS STIG	- Added Section 1.7 Product Approval Disclaimer to the STIG Overview document. - V-1080 - Removed requirement due to excessive event generation. - V-1088 - Removed requirement due to excessive event generation. - V-1118 - Increased Security event log size to 196608 KB or greater. - 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-6850 - Removed object access audit requirements due to excessive event generation. - V-14226 - Removed references to SAMI data. - V-15671 - Removed requirement preventing root certificate updates from Microsoft. - V-26070 - Clarified requirement to maintain the default permissions. - V-32282 - Clarified requirement to maintain the default permissions. - V-36669 - Removed requirement due to excessive event generation. Windows 2008 MS Benchmark, V6R34: - V-1080 - Disabled Rule. - V-1081 - Added OVAL. - V-1118 - Modified OVAL to change MaxSize value to 196608. - V-1155 - Modified the OVAL to include an equals check for the Enterprise Admins group.	22 April 2016

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-6850 - Modified the OVAL to no longer check for the audit subcategories File System and Registry to match the updated STIG. - 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 an equals check for the Enterprise Admins group. 	
V6R31	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - V-1074 - Removed Symantec from requirement. - V-1077 - Updated to allow default permissions. - V-1103 - Updated "Manage auditing and security log" user right to allow "Administrators". - V-1137 - Removed 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. <p>- 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-4444.</p> <p>- Removed EMET requirements: V-36701, V-36702, V-36703, V-36704, V-36705, V-36706, V-39137</p> <p>Windows 2008 MS Benchmark, V6R33:</p> <ul style="list-style-type: none"> - V-1103 Updated "Manage auditing and security log" user right: Allow "Administrators". - V-15823 Matched file extensions case insensitivity. 	23 October 2015

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - 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 an additional path for the certificate. - Removed unreferenced OVAL content. 	
V6R30	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - Added Section 1.6 Other Considerations to the STIG Overview document. - V-3385 - Corrected policy name. - V-39137 - Updated to require EMET v5.x. Support for v4.x ended 09 June 2015. <p>Windows 2008 MS Benchmark, V6R32:</p> <ul style="list-style-type: none"> - V-1099 Modified check for account lockout policy. - 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-32272 Added registry check. - V-32274 Added registry check. - V-39137 Updated check for EMET. 	24 July 2015
V6R29	- Windows 2008 MS STIG	<ul style="list-style-type: none"> - The STIG version number has been modified to remove "1" from release number. - STIG Support Helpdesk email has been updated to disa.stig_spt@mail.mil. - DISA Field Security Operations (FSO) changed to DISA. - V-1090 - Requirement is NA for non domain joined systems. 	24 April 2015

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-4108 - Changed from Documentable to NA if audit records are written directly to an audit server. - V-15680 - Requirement is NA for domain joined systems, retargeted to member servers only. - V-15719 - Requirement is NA for non domain joined systems. - EMET - The following requirements are applicable to unclassified systems: - V-39137 - Requirement to have EMET installed changed to a CAT I. Note added regarding end of support for V4.x in June 2015. - V-36701, V-36702, V-36703, V-36704, V-36705, V-36706. Windows 2008 MS Benchmark, V6R31: - V-1090 added applicability statement. - V-1098 added OVAL check for Lockout Threshold. - V-1099 added OVAL check for Lockout Threshold. - V-15680 applicability statement will be added; setting is NA for domain systems. - V-15719 added applicability statement. - V-15823 OVAL updated to improve efficiency. - V-56511 added to benchmark. - V-57455 added to benchmark. - V-57463 added to benchmark. - V-57465 added to benchmark. - V-57467 added to benchmark. - V-57469 added to benchmark. - V-57471 added to benchmark. - V-57473 added to benchmark. - V-57475 added to benchmark. - V-57477 added to benchmark. - V-57479 added to benchmark. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- Added XCCDF profile to exclude intensive checks when used on systems with a large number of user accounts.	
V6R1.28	- Windows 2008 MS STIG	<p>- STIGs previously bundled in the Windows Server packages have been separated into individual packages (e.g., Member Server, Domain Controller, AD Domain, and AD Forest).</p> <p>- Windows Error Reporting requirements have been updated/added to enable error reporting and maintain locally. STIG IDs have been updated to organize the requirements.</p> <p>- V-3471 - Error Reporting - Removed, replaced by V-15715.</p> <p>- V-15714 - Error Reporting - Logging - Updated Severity.</p> <p>- V-15715 - Error Reporting - Updated to enable error reporting.</p> <p>- V-15717 - Error Reporting - Additional Data - Updated to enable.</p> <p>- V-56511 - Error Reporting - Service - Added.</p> <p>- V-57455 - Error Reporting - Inhibit User Notifications - Added.</p> <p>- V-57457 - Error Reporting - Configure Reporting Server Name - Added.</p> <p>- V-57459 - Error Reporting - Configure Secure Sockets Layer (SSL) - Added.</p> <p>- V-57461 - Error Reporting - Configure Reporting Port Number - Added.</p> <p>- V-57463 - Error Reporting - Enable Report Archive - Added.</p> <p>- V-57465 - Error Reporting - Configure Report Archive - Added.</p> <p>- V-57467 - Error Reporting - Maximum Archived Reports - Added.</p> <p>- V-57469 - Error Reporting - Enable Error Queuing - Added.</p> <p>- V-57471 - Error Reporting - Queuing Behavior - Added.</p>	23 January 2015

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-57473 - Error Reporting - Maximum Queued Reports - Added. - V-57475 - Error Reporting - Queue Reporting Interval - Added. - V-57477 - Error Reporting - Configure Default Consent - Added. - V-57479 - Error Reporting - Configure Consent Overrides - Added. <p>- The following requirements have been updated to account for changes in the group name to assign deny rights to local administrator accounts:</p> <ul style="list-style-type: none"> - V-1155 - Deny Access from the Network. - V-26486 - Deny log on through Remote Desktop \ Terminal Services. - V-45589 - Define group for deny rights. <p>- V-14253 - RPC - Unauthenticated RPC Clients - Retargeted to member servers only.</p> <p>- V-14262 - IPv6 Transition - Updated with additional registry value.</p> <p>- V-15682 - RSS Attachment Downloads - Removed references to XP.</p> <p>Windows 2008 MS Benchmark, V6R1.30:</p> <ul style="list-style-type: none"> - V-1113 - Revised pattern match for the Built-in Guest account SID to resolve false positives. - V-1114 - Revised pattern match for the Built-in Guest account SID to resolve false positives. - V-1115 - Revised pattern match for the Built-in Admin account SID to resolve false positives. - V-1155 - Revised OVAL content to allow for the "DeniedNetworkAccess" group. Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-3338 - Revised OVAL content to allow for the "Anonymous Access to Named Pipes" policy setting to be blank. - V-14262 - Revised OVAL content to allow for an alternate value. - V-15715 - Revised OVAL content to require the "Disable Windows Error Reporting" setting to be disabled. - V-15717 - Revised OVAL content to require the "Do not send additional data" setting to be disabled. - V-26483 - Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26484 - Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26485 - Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26486 - Revised OVAL content to allow for the "DeniedNetworkAccess" group. Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-32272 - Added OVAL content for the "DoD Root Certificate" requirement. - V-32274 - Added OVAL content for the "DoD Interoperability Root CA 1 to DoD Root CA 2 cross-certificate" requirement. - V-40237 - Added OVAL content for the "US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate" requirement. - V-45589 - Revised OVAL content to allow for the "DeniedNetworkAccess" group. 	
V6R1.27	- Windows 2008 STIG	- Control Correlation Identifiers (CCIs) added to requirements.	28 October 2014

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - EMET requirements have been changed back to CAT II. EMET V4.1 Update 1 or later required. - V-39137 EMET must be installed on the system. - V-36701 EMET ASLR must be enabled. - V-36702 EMET default protections for IE must be enabled. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled. - V-36705 EMET Data Execution Prevention must be enabled. - V-36706 EMET SEHOP must be enabled. <p>Benchmark\Oval Updates:</p> <ul style="list-style-type: none"> - Oval for EMET updated based on requirement for EMET V4.1 Update 1. - V-39137 EMET must be installed on the system. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled. 	
V6R1.26	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-1074 Approved DoD Virus Scan Program - Removed Gold Disk references. - V-1126 Recycle Bin Configuration - Removed Gold Disk references. - V-1128 Security Configuration Tools - Removed Gold Disk references. - V-1136 Forcibly Disconnect When Logon Hours Expire - Removed Gold Disk references. - V-1168 Members of Backup Operators Group - Typo correction in Vulnerability Discussion. - V-3245 File Shares - Typo correction in Check. - V-4444 Strong Key Protection - Typo correction in Vulnerability Discussion. 	25 July 2014

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-6836 Minimum Password Length - Fix detail added, correcting typo. - V-14262 IPv6 Transition - Removed Gold Disk references. - V-15672 Event Viewer Links - Typo correction in Rule Title. - V-16006 Unnecessary Features - Typo correction in Check. - V-36439 Local Admin Accounts Filtered Token Policy - Retargeted to member servers only, not applicable to domain controllers. <p>Benchmark/Oval Updates:</p> <ul style="list-style-type: none"> - V-34974 - Added OVAL content for the requirement. 	
V6R1.25	- Windows 2008 STIG	<ul style="list-style-type: none"> - EMET requirements have been changed to CAT IV, pending further resolution. - V-39137 EMET must be installed on the system. - V-36701 EMET ASLR must be enabled. - V-36702 EMET default protections for IE must be enabled. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled. - V-36705 EMET Data Execution Prevention must be enabled. - V-36706 EMET SEHOP must be enabled. - V-15712 Search - Exchange Folder Indexing - Removed from STIG, applicable to workstations. <p>Member Server Specific Requirements:</p> <ul style="list-style-type: none"> - V-1155 Deny access from the network - Updated to incorporate "DenyNetworkAccess" group defined in V-45589. - V-26486 Deny log on through Terminal Services - Updated to incorporate 	25 April 2014

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>"DenyNetworkAccess" group defined in V-45589.</p> <ul style="list-style-type: none"> - V-45589 - New - A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. <p>Benchmark/Oval Updates:</p> <ul style="list-style-type: none"> - V-36703 Updated content to use variable checks in lieu of multiple tests. - V-36704 Updated content to use variable checks in lieu of multiple tests. - V-36705 Updated content to allow for "Always On" for Data Execution Prevention. - V-39137 Updated content to verify EMET version using the registry in lieu of the version of the EMET DLL file. <p>Member Server Specific Requirements:</p> <ul style="list-style-type: none"> - V-1155 Added automated content for the vulnerability. - V-26846 Added automated content for the vulnerability. - V-45589 Added automated content for the vulnerability. 	
V6R1.24	- Windows 2008 STIG	<ul style="list-style-type: none"> - BIOS requirements added to STIG: - V-36663 Admin password. - V-36664 Removable Media, CAT I. - V-40195 User-level access. <ul style="list-style-type: none"> - PKE requirements updated to define applicable network: - V-32272 DoD Root Certificate. - V-32274 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate - Check updated with new thumbprint. - V-40237 DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate. - V-32273 External CA Root Certificate - Removed from STIG. 	24 January 2014

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>- V-15996 TS/RDS Clipboard Redirection - Removed from STIG.</p> <p>Benchmark/Oval Updates:</p> <p>- V-1113 Disable Guest Account - Updated OVAL content to check for the SID instead of the account name.</p> <p>- V-1114 Rename Built-in Guest Account - Updated OVAL content to check for the SID instead of the account name.</p> <p>- V-1115 Rename Built-in Administrator - Updated OVAL content to check for the SID instead of the account name.</p> <p>- V-15823 Software Certificate Installation Files - Content was previously removed from the benchmark due to an issue when using SCC. The issue has been corrected.</p>	
V6R1.23	- Windows 2008 STIG	<p>- The following sections were removed from the Overview document. Deviations or exceptions must follow standard adjudication process. IAVMs are no longer included with Windows STIGs.</p> <p>3.2 ACL Deviations</p> <p>3.3 Application Exceptions</p> <p>3.4 IAVM Checks</p> <p>- V-3480 Media Player Disable Automatic Updates - typo correction in Vulnerability Discussion.</p> <p>- V-6850 Auditing Configuration - separated to address member server vs. domain controller requirements. SV-16967 Member Server, SV-51984 Domain Controller.</p> <p>- V-16007 8dot3 Name Creation - removed from STIGs.</p> <p>- V-14228 Audit Access of Global System Objects - policy name correction.</p> <p>- V-32274 DoD Interop Root CA 1 to DoD Root CA 2 cross cert - updated with new certificate information from PKE.</p> <p>- V-36701 EMET System ASLR - updated to include V4.0 policy name change.</p>	25 October 2013

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-36705 EMET System DEP - updated to include V4.0 policy name change. - V-36706 EMET System SEHOP - updated to include V4.0 policy name change. - V-40237 US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate - new cross cert requirement from PKE. - Readme.txt file - removed references to FOUO version of STIG no longer produced. Benchmark/Oval Updates: <ul style="list-style-type: none"> - V-6850 Auditing Configuration - removed unnecessary extended definitions and removed test for "No Auditing" entries. - V-16007 8dot3 Name Creation - removed from benchmark. - V-36701 EMET ASLR Configuration - content added for the requirement. - V-36702 EMET Default Protections for IE - content added for the requirement. - V-36703 EMET Default Protections for Recommended Software - content added for the requirement. - V-36704 EMET Default Protections for Popular Software - content added for the requirement. - V-36705 EMET System-wide DEP Configuration - content added for the requirement. - V-36706 EMET System-wide SEHOP Configuration - content added for the requirement. - V-39137 EMET must be installed - content added for the requirement. 	
V6R1.22	- Windows 2008 STIG	<ul style="list-style-type: none"> - Section on the Enhanced Mitigation Experience Toolkit (EMET) added to the Overview document. - V-1145 Disable Automatic Logon - updated to Cat II with Cat I severity override. 	26 July 2013

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-4448 Group Policy - Registry Policy Processing - corrected GUID referenced in note. - V-14235 UAC - Admin Elevation Prompt - updated requirement to align with Windows 2008 R2 STIG. - V-36669 The system must be configured to audit Object Access - Handle Manipulation failures - added requirement. - Requirements added for Enhanced Mitigation Experience Toolkit (EMET): - V-39137 EMET must be installed on the system. - V-36701 EMET system-wide Address Space Layout Randomization (ASLR) must be enabled and configured. - V-36702 EMET Default Protections for Internet Explorer must be enabled. - V-36703 EMET Default Protections for Recommended Software must be enabled. - V-36704 EMET Default Protections for Popular Software must be enabled. - V-36705 EMET system-wide Data Execution Prevention (DEP) must be enabled and configured. - V-36706 EMET system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be enabled and configured. Benchmark/Oval Updates: - CPE definition updated to account for "Windows 2008 without Hyper-V" versions. - V-3340 Anonymous Access to Network Shares - updated to allow blank registry value or no registry value at all. - V-15823 Software Certificate Installation Files – removed from benchmark. - V-14235 UAC - Admin Elevation Prompt - updated requirement to align with Windows 2008 R2 STIG. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - Corrected several CCEs referenced in OVAL: Def:2133 - CCE-2078-4. Def:2134 - CCE-2506-4. Def:2099 - CCE-2075-0 (Member Server). 	
V6R1.21	- Windows 2008 STIG	<ul style="list-style-type: none"> - IAVMs are no longer incorporated in an FOUO version of the Windows STIGs. They will be produced as IAVM STIGs for the specific Windows versions. - V-34974 Always Install with Elevated Privileges Disabled - new Cat I requirement. - Pass the Hash/Credential Theft Mitigations: Requirements have been added or updated to mitigate Pass the Hash/Credential Theft attacks in domains. Requirements may vary between Domain Controllers and Member Servers where noted. - A section on this with a reference to a Microsoft document has been added to the STIG Overview document. - V-1140 Users with Administrative Privilege - changed to Cat I. - V-36451 Accounts with administrative privileges internet access - new Cat I. - V-36439 Built-in admin accounts filtered token enabled - new Cat II. <p>Member Server Specific Requirements:</p> <ul style="list-style-type: none"> - V-1127 Restricted Administrator Group Membership - changed to a Cat I, retargeted existing Rule ID to member servers, added requirement for domain member server administrator group on domain systems. - Several User Rights have been updated, restricting Domain and Enterprise Admins groups and/or local administrator accounts on 	29 March 2013

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>domain systems. Ones that had been part of a combined User Rights requirement (V-1103) have been separated to individual requirements.</p> <ul style="list-style-type: none"> - V-1155 Deny Access from the Network - Rule ID retargeted to Member Servers, requirement updated. STIG ID changed to WINUR-000017-MS. - V-1103 User Rights Assignments - removed the following User Rights. - V-26483 Deny log on as a batch job - STIG ID WINUR-000018-MS. - V-26484 Deny log on as a service - STIG ID WINUR-000019-MS. - V-26485 Deny log on locally - STIG ID WINUR-000020-MS. - V-26486 Deny log on through Terminal Services - STIG ID WINUR-000021-MS. <p>Benchmark/Oval Updates: Member Server Specific Requirements: The following were removed.</p> <ul style="list-style-type: none"> - V-1155 User Right - Deny access from the network. - V-1103 Extended definitions for User Rights - Deny log on as a service and Deny log on locally. 	
V6R1.20	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-1089 Legal Banner - corrected double dash in banner text. - V-32272 DoD Root Certificate - add reference for PKE Tools to Fix section. - V-32273 ECA Root Certificate - add reference for PKE Tools to Fix section. - V-32274 DoD Interoperability Root CA to DoD Root CA 2 cross cert - add reference for PKE Tools to Fix section. - Various editing corrections. 	26 October 2012
V6R1.19	- Windows 2008 STIG	<ul style="list-style-type: none"> - Overview Section 1.6 - updated email address for FSO STIG Customer Support. - New Cat I Requirement: 	27 July 2012

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-32282 Active Setup Registry Permissions. - 3 new PKE requirements added: - V-32272 DoD Root Certificate. - V-32273 ECA Root Certificate. - V-32274 DoD Interoperability Root CA to DoD Root CA 2 cross cert. - V-1088 Registry Key Auditing - corrected reference to Object Auditing requirement to V-6850. - V-3469 Group Policy - Do Not Turn off Background Refresh - check clarification. - V-26359 Legal Banner Dialog Box Title - updated for consistency and clarification. Two predefined titles, clarification on site defined titles. <p>Benchmark\Oval Updates:</p> <ul style="list-style-type: none"> - V-26359 Legal Banner Dialog Box Title - updated to test for two predefined titles. <p>CPE OVAL changed to FSO namespace, test for ProductName instead of ProductVersion.</p>	
V6R1.18	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-1089 Legal Notice - corrected registry type referenced to reg_sz. <p>Benchmark\Oval Updates:</p> <ul style="list-style-type: none"> - V-1103 User Rights - updated, added back to benchmark. - Various CCE references added. 	27 April 2012
V6R1.17	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-1130 System Files ACLs - added Documentable flag consistent with other Windows STIGs. - V-3373 Maximum Machine Account Password Age - updated for clarification, 0 is not a valid option. - V-3457 TS/RDS Time Limit for Discontinued Session - updated for clarification, changed from 1 or less to equals 1. 	27 January 2012

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-3458 TS/RDS Time Limit for Idle Session - updated for clarification, 0 is not a valid option. - V-3471 Error Reporting - corrected policy path in Documentable section. - V-3472 Windows Time Service NTP - updated for clarification. - V-4438 TCP Data Retransmissions - corrected registry path, removed duplicate "system". - V-4448 Group Policy Registry Policy Processing - correction removing secondary registry check. <p>Benchmark\Oval Updates:</p> <ul style="list-style-type: none"> - V-1089 Legal Notice - updated to support Policy Auditor 5.3. - V-1157 Smart Card Removal Option - corrected to allow for "1" or "2". - V-3339 Remotely Accessible Registry Paths - updated to account for blank. - V-3373 Maximum Machine Account Password Age - updated to exclude "0". - V-3457 TS/RDS Time Limit for Discontinued Session - updated from 1 or less to equal 1. - V-3458 TS/RDS Time Limit for Idle Session - updated to exclude "0". - V-3472 Windows Time Service NTP - removed, manual check. - V-4443 Remotely Accessible Registry Paths & Subpaths - updated to account for blank. - V-4448 Group Policy Registry Policy Processing - correction removing secondary registry check. - V-6840 Password Expiration - removed, manual check. - V-7002 Password Requirement - removed, manual check. - V-15823 Certificate Installation Files - updated to search all local drives. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-17900 Disallow Autorun.inf - updated to accommodate capitalization variations.	
V6R1.16	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-6840 Password Expiration - exception added for domain accounts that require smart card. - V-7002 Password Requirement - exception added for domain accounts that require smart card. - V-1077 Event Log ACLs - added clarification to Fix on configuration of Eventlog account. 	28 October 2011
V6R1.15	- Windows 2008 STIG	<ul style="list-style-type: none"> - V-1073 Service Packs - Service Packs prior to SP2 are unsupported effective 12 July 2011 and a Cat I. Updated to change focus to Cat I unsupported service packs vs. Cat II required service packs. - V-1089 Legal Notice - Caption/Title setting moved to separate requirement. V-26359 Legal Banner Title. - V-15505 HBSS McAfee Agent - updates to reflect current requirements. - Platinum only requirements changed to "Both", Gold and Platinum: V-3382, V-3383, V-3666, V-6832, V-6833. - V-3382, V-3666 Corrected registry path referenced to "CurrentControlSet\Control". Benchmark\Oval Updates: <ul style="list-style-type: none"> - V-1089, V-26359 - Legal Notice update, caption/title moved to separate check. - V-1093 Account Lockout Threshold - corrected to check for a value less than or equal to 3 but not 0. 	29 July 2011
V6R1.14	- Windows 2008 STIG	<ul style="list-style-type: none"> - NEW CAT I Requirement: - V-26070 Winlogon registry permissions. - Removed - not applicable: 	29 April 2011

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - V-14267 Power Mgmt - Require Password on Resume. - V-15669 Prohibit Internet Connection Sharing. - V-14262 IPv6 - Correction to 0xffffffff to disable all interfaces due to discrepancies in supporting documentation. - The following requirements were updated to add registry information to the Checks and/or policy information to the Fixes. Additional updates noted where applicable. (The requirements themselves have not changed.): - V-1075, V-1093, V-1153, V-1158, V-1159, V-1173, V-3338, V-3339, V-3340, V-3376, V-3377, V-3378, V-3379, V-3381, V-3382, V-3383, V-3385, V-3666, V-4108, V-4438, V-4442, V-4443, V-6834, V-4444, V-4445, V-4446, V-14234, V-14235, V-14236, V-14237, V-14239, V-14240, V-14241, V-14242, V-15991, V-16008. - Various - References to unsupported OS versions, the Windows Addendum and specific organizations removed. Spelling corrections with no impact to requirements. - Overview Document - Removed section on Gold/Platinum policies. Platinum only requirements will be changed to both with next release. Added section on IAVM checking. <p>Benchmark\Oval Updates:</p> <ul style="list-style-type: none"> - The Windows 2008 Benchmark was updated for the removal of V-15669 and change to V-14262. 	
V6R1.13	- Windows 2008 STIG	- V-3245 File Share ACLs - corrected typo in Check "regular".	31 December 2010

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>- The following requirements were updated to add registry information to the Checks and/or policy information to the Fixes. Additional updates noted where applicable. (The requirements themselves have not changed.):</p> <p>- V-1090, V-1136, V-1141, V-1145, V-1151, V-1154, V-1157, V-1162, V-1163, V-1164, V-1165, V-1166, V-1171, V-1172, V-1174, V-3344, V-3372, V-3373, V-3374, V-3479 (corrected policy name to match current Security Options), V-4110, V-4111, V-4112 (corrected "IRDP" in Check), V-4113 (corrected policy name to match current Security Options), V-4116, V-6831, V-6832, V-6833, V-11806, V-14228, V-14229, V-14230, V-14232, V-16007.</p>	
V6R1.12	- Windows 2008 STIG	<p>- V-1089 Legal Notice is not configured - removed False Positive note from VMS. Banner must be configured exactly as stated. Removed "," (comma) after COMSEC. Corresponding update made in "Analyze_only" security template.</p> <p>- V-1131 Strong Password Filtering - Updated to clarify enpasflt.dll is provided as an option but must be tested in particular environments. Site is responsible for having password complexity software.</p> <p>- V-2907 System File Changes - added note on HBSS FIM meeting requirement.</p> <p>- V-14262 IPv6 Transition - corrected registry value for disabling all interfaces to 0xFF.</p>	27 August 2010