APRIL 2017 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Apple iOS 10 STIG, Version 1, Release 3

V-71887

Requirement was removed because the device must be in supervised mode for the MDM to set the configuration. Supervised mode is not currently a STIG requirement.

Documentation Update

Revised Configuration Tables document:
-updated the applicable STIGID number for the policy rule "App must be deleted when the MDM enrollment profile is removed"
-removed policy rule "Remove managed applications upon unenrollment from MDM" because it was duplicative of another policy rule

Apple OS X 10.10 Workstation STIG, Version 1, Release 5

Documentation Update

Restored configuration profiles to the STIG bundle.

Apple OS X 10.11 STIG, Version 1, Release 4

V-67617

Updated mobileconfig profile to match manual STIG content, specifically SPConfigurationProfileDataType to return 1.

Application Security and Development STIG, Version 4, Release 3

V-70189

Remove reference to Suite B in vul discussion.

V-70191

Remove reference to SHA1 and SHA2 in Fix.

V-70193

Change NSS language in vul discussion from SHA-256 to SHA-384.

CA API Gateway ALG STIG, Version 1, Release 2

V-71325

Update the If statement in the Check Content. Change to "If the "security.fips.enabled" property is not listed or is set to false this is a finding." It previously said True which does not match V-71325 and is technically inaccurate.

Defense RED Switched Network (DRSN) STIG, Version 1, Release 7

Documentation Update

Move VVoIP 5310 (V-19654) to the Voice Video Services Policy STIG.

Defense Switched Network (DSN) STIG, Version 2, Release 8

Documentation Update

Move VVoIP 5310 (V-19654) to the Voice Video Services Policy STIG.

EDB Postgres Advanced Server STIG, Version 1, Release 3

V-68887

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68889

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68891

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68893

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68895

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68897

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68899

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68901

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68903

Reworded Check and Fix to give users more flexibility in configuring audit.

V-68905

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69007

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69027

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69029

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69031

Reworded Check and Fix to give users more flexibility in configuring audit.
Rule Title corrected.

V-69033

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69035

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69037

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69039

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69041

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69043

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69045

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69047

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69049

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69051

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69053

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69055

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69057

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69059

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69061

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69063

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69065

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69067

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69069

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69071

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69073

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69075

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69087

Reworded Check and Fix to give users more flexibility in configuring audit.

V-69089

Reworded Check and Fix to give users more flexibility in configuring audit.

F5 BIG-IP Device Management 11.x STIG, Version 1, Release 4

V-60093

Changed requirement from 900 Seconds (15 minutes) to 600 seconds (10 minutes) to coincide with the setting in F5BI-DM-000137.

Google Chrome Benchmark, Version 1, Release 3

Benchmark Update

Updated Google Chrome Benchmark CPE to recognize varying install points in the registry.

Google Chrome STIG, Version 1, Release 8

V-44757

Modify rule requirement to state "3D Graphics APIs must be disabled if not needed".

HBSS ePO 5.x STIG, Version 1, Release 12

V-31358

Expand on check content regarding "sys account".

HBSS HIP 8 Firewall STIG, Version 1, Release 8

V-47483

Elaborate on the vulnerability discussion to support need for enforcing a rule to explicity allow outbound connections.

V-47485

Correct Network Protocol from IPV6 to IPV4.

HBSS HIP 8 STIG, Version 4, Release 19

V-14532

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14536

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14537

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14540

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14541

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14543

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14544

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14546

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14547

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14548

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-14560

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-17891

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-17893

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-31085

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-31086

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-43197

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-43199

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-43200

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-43201

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-55659

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-55661

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-55663

Modify Check Content steps to accurately validate effective policies on asset being checked.

V-60665

Remove duplicate signature references that are accounted for in other STIG IDs.

V-60667

Remove duplicate signature references that are accounted for in other STIG IDs.

V-60669

Remove duplicate signature references that are accounted for in other STIG IDs.

HBSS McAfee Agent STIG, Version 4, Release 13

V-43051

Clarification regarding application scan tool.

IIS 7.0 Site STIG, Version 1, Release 13

V-3333

Add verbiage for exception, allowing ISSO to grant a risk acceptance.

V-6577

Expand on requirement to ensure only required services are running.

V-13689

Clarify permissions on web-site log files.

Infoblox 7.x DNS STIG, Version 1, Release 3

V-68613

Add allowance for those not using a split DNS configuration.

V-68615

Add allowance for those not using a split DNS configuration.

JBoss EAP 6.3 STIG, Version 1, Release 2

V-62321

The STIG specifies "ls /subsystem=web/connector=http/ssl=" correct command is: "ls /subsystem=web/connector=HTTPS/ssl=configuration".

V-62323

The STIG specifies "ls /subsystem=web/connector=http/ssl=" correct command is: "ls /subsystem=web/connector=HTTPS/ssl=configuration".

McAfee VirusScan88 Local Client STIG, Version 5, Release 13

V-42559

Correct finding statement for the "Prevent execution of scripts from the Temp folder" option.

McAfee VirusScan88 Managed Client STIG, Version 5, Release 15

V-42526

Correct finding statement for the "Prevent execution of scripts from the Temp folder" option.

Microsoft Access 2013 STIG, Version 1, Release 5

V-72833

Removed requirement added in error; not applicable to this Office module.

Microsoft Exchange 2013 Mailbox STIG, Version 1, Release 2

V-69955

Bring the Check and Fix content in sync regarding the Get-TransportService command.

V-69957

Bring the Check and Fix content in sync regarding the Get-TransportService command.

V-69997

Correction to syntax of Get-Mailbox criteria to validate Exchange email forwarding restriction.

Microsoft IE 10 Benchmark, Version 1, Release 9

Benchmark Update

Generated new IE10 Benchmark to go along with requirement Rule ID revision number incremental increase due to manual STIG update. No OVAL content modifications necessary.

Microsoft IE10 STIG, Version 1, Release 15

V-6238

Correction to registry key value.
Modify requirements to TLS 1.1 or above, in compliance with NIST 800-52.

V-22108

Marking STIG ID to be Not Applicable if on Classified network.

Microsoft Office Excel 2013 Benchmark, Version 1, Release 4

V-72831

Added new OVAL content for the requirement coinciding with the addition of the requirement to the manual STIG for the January 2017 Release.

Microsoft Office Outlook 2010 Benchmark, Version 1, Release 3

V-26625

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

Microsoft Office PowerPoint 2013 Benchmark, Version 1, Release 3

V-72839

Added new OVAL content for the requirement coinciding with the addition of the requirement to the manual STIG for the January 2017 Release.

Microsoft Office Word 2013 Benchmark, Version 1, Release 3

V-72829

Added new OVAL content for the requirement coinciding with the addition of the requirement to the manual STIG for the January 2017 Release.

Microsoft Outlook 2013 STIG, Version 1, Release 10

V-72837

Removed requirement added in error; not applicable to this Office module.

Microsoft SQL Server 2014 Database STIG, Version 1, Release 4

V-67423

Corrected audit action name in Check query.

V-67425

Corrected audit action name in Check query.

V-67431

Corrected audit action name in Fix query.

V-67433

Corrected audit action name in Fix query.

Documentation Update

Comment modified in the Audit.sql script file, to note an equivalence between DATABASE_OBJECT_ACCESS_GROUP and Trace Event 180. No change to STIG text. [Many other requirements also refer to this script, but none need editing.]

Microsoft SQL Server 2014 Instance STIG, Version 1, Release 5

V-67787

Clarification of the use of the is_rollover parameter in a Trace-based audit.

V-67903

Corrected duplication of DATABASE_OWNERSHIP_CHANGE_GROUP in queries.

Documentation Update

Comment modified in the Audit.sql script file, to note an equivalence between DATABASE_OBJECT_ACCESS_GROUP and Trace Event 180. No change to STIG text. [Many other requirements also refer to this script, but none need editing.]

Microsoft Windows 2012 Server Domain Name System STIG, Version 1, Rele

V-58579

Modify Check Content to reflect scenario of DNS on Classified network.

V-58581

Modify Check Content to reflect scenario of DNS on Classified network.

V-58585

Modify vulnerability/check/fix content to provide clarity regarding the possible use of name servers for blackhole.

V-58615

Modify Check Content to reflect scenario of DNS on Classified network.

V-58671

Correct vulnerability discussion and check/fix content to reflect that DS records must be present but are not added by DNSSEC signing and are added manually.

Documentation Update

Add verbiage to Overview regarding Blackhole name servers WRT DNSSEC.

Mozilla Firefox STIG, Version 4, Release 18

V-6318

Clarify check criteria to be not applicable if using SHA2 algorithm.

V-15983

"security.tls.version.min" is set to the value "2" and locked, in compliance with NIST 800-52.

Network Device Management SRG, Version 2, Release 8

V-55037

Removed requirement for two or more authentication servers because this was deemed to be overly burdensome. Use account of last resort when network access or authentication server is not available.

Network Firewall STIG - Cisco, Version 8, Release 22

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-3054

Updated check to align with newer firewall appliances.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

Network Firewall STIG, Version 8, Release 22

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-3054

Updated check to align with newer firewall appliances.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

Network Infrastructure L3 Switch STIG - Cisco, Version 8, Release 22

V-7009

Updated entire check - replaced EIGRP and RIP with IGP, removed MD5 Key reference, and changed key expiration value. Removed Information Assurance Officer from Responsibility.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Infrastructure L3 Switch STIG, Version 8, Release 22

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Infrastructure Policy STIG, Version 9, Release 3

V-31637

Removed CNSSI reference from Discussion.

Network Infrastructure Router STIG - Cisco, Version 8, Release 22

V-7009

Updated entire check - replaced EIGRP and RIP with IGP, removed MD5 Key reference, and changed key expiration value. Removed Information Assurance Officer from Responsibility.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Infrastructure Router STIG - Juniper, Version 8, Release 22

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Infrastructure Router STIG, Version 8, Release 22

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network IPSec VPN Gateway STIG, Version 1, Release 12

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30959

Updated Diffie-Hellman requirement from Group 2 or higher to Group 14 or higher.

V-30963

Updated Diffie-Hellman requirement from Group 2 or higher to Group 14 or higher.

Network Perimeter L3 Switch STIG - Cisco, Version 8, Release 25

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-7009

Updated entire check - replaced EIGRP and RIP with IGP, removed MD5 Key reference, and changed key expiration value. Removed Information Assurance Officer from Responsibility.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Perimeter L3 Switch STIG, Version 8, Release 25

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Perimeter Router STIG - Cisco, Version 8, Release 25

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-7009

Updated entire check - replaced EIGRP and RIP with IGP, removed MD5 Key reference, and changed key expiration value. Removed Information Assurance Officer from Responsibility.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Perimeter Router STIG - Juniper, Version 8, Release 25

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Perimeter Router STIG, Version 8, Release 25

V-3005

Check was removed as it was no longer relevant and does not provide any security advantage.

V-14667

Updated entire check to ensure rotating keys are set to expire at 180 days or less. Removed Information Assurance Officer from Responsibility.

V-30585

Check was removed as it was no longer relevant and does not provide any security advantage.

Network Removable Storage and External Connections STIG, Version 1, Rele

V-22112

Updated entire check and removed reference to NSA-approved wipe tools and website.

Oracle Database 11.2g STIG, Version 1, Release 11

V-52141

Check: provided more detail on how to check DBMS settings to determine whether system state information is being preserved in the event of a system failure.

V-52163

Check: reworded text on checking if real-time alerts are being sent upon auditing failure. Discussion and Fix: Added mention of Oracle Enterprise Manager.

V-52167

Check: removed reference to "DBMS," as the required functionality is not part of Oracle Database, and must be sourced externally. Fix: Added mention of Oracle Enterprise Manager.

V-52171

Reworded Rule Title, Discussion, Check and Fix to acknowledge that audit trail reduction is not provided by Oracle, and must be sourced externally.

V-52245

Rule Title: Modified to make clear that this is a requirement that backups must actualy be done.
Check: added mention of V$RMAN_STATUS view.

V-52297

Added information on non-default locations for FIPS.ora.

V-52379

Check: provided more detail on how to review user privileges to system tables and configuration data stored in the database.

V-52387

Check: provided more detail on how to review permissions for objects owned by DBA or other administrative accounts.

V-52393

Check: provided more detail on how to review access permissions for objects owned by application owners or other non-administrative users.

V-52399

Check: provided more detail on how to validate that OS accounts used by the DBMS have only the privileges necessary to perform the required functionality.

V-53967

Severity lowered to Category III.

V-54017

Check query modified to achieve the desired result of excluding accounts which only own synonyms.

V-54035

Non-SRG requirement removed.

V-54053

Non-SRG requirement removed. Oracle informs us that there is really no way to do this using Oracle's technical features.

Oracle Database 12c STIG, Version 1, Release 7

V-61417

Severity lowered to Category III.

V-61467

Check query modified to achieve the desired result of excluding accounts which only own synonyms.

V-61505

Non-SRG requirement removed.

V-61521

Non-SRG requirement removed. Oracle informs us that there is really no way to do this using Oracle's technical features.

V-61589

Check: provided more detail on how to review user privileges to system tables and configuration data stored in the database.

V-61593

Check: provided more detail on how to review permissions for objects owned by DBA or other administrative accounts.

V-61599

Check: provided more detail on how to review access permissions for objects owned by application owners or other non-administrative users.

V-61601

Check: provided more detail on how to validate that OS accounts used by the DBMS have only the privileges necessary to perform the required functionality.

V-61645

Check: reworded text on checking if real-time alerts are being sent upon auditing failure. Discussion and Fix: Added mention of Oracle Enterprise Manager.

V-61647

Check: removed reference to "DBMS," as the required functionality is not part of Oracle Database, and must be sourced externally. Fix: Added mention of Oracle Enterprise Manager.

V-61649

Reworded Discussion, Check and Fix to acknowledge that audit trail reduction is not provided by Oracle, and must be sourced externally.

V-61693

Rule Title: Modified to make clear that this is a requirement that backups must actualy be done. Check: added mention of V$RMAN_STATUS view.

V-61747

Added information on non-default locations for FIPS.ora.

V-61759

Added information on non-default locations for FIPS.ora.

V-61769

Check: provided more detail on how to check DBMS settings to determine whether system state information is being preserved in the event of a system failure.

Oracle JRE 8 UNIX STIG, Version 1, Release 2

V-66925

Modify check and fix criteria to remove the "file:// ".

Oracle Linux 5 STIG, Version 1, Release 10

V-782

Adjusted the requirement to support OPORD 16-0080.

V-22427

Removed "sys" and "system" as authorized group-owners for the /etc/services file.

Oracle Linux 6 STIG, Version 1, Release 10

V-50535

Updated finding statement to allow for documented changes due to STIG application.

V-50591

Updated finding statement to allow for documented changes due to STIG application.

V-50593

Updated finding statement to allow for documented changes due to STIG application.

V-50617

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-50875

Adjusted the requirement to support OPORD 16-0080.

V-50955

Adjusted the check to lessen the ambiguity between the “long” and “short” versions of the banner.

V-50989

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-50997

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-51005

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-51111

Updated the finding statement to only accept “/bin/true” as a valid setting.

Red Hat 5 STIG, Version 1, Release 18

V-782

Adjusted the requirement to support OPORD 16-0080.

V-22427

Removed "sys" and "system" as authorized group-owners for the /etc/services file.

Red Hat 6 Benchmark, Version 1, Release 15

V-38476

Added OVAL to ensure Red Hat cryptographic keys are installed.

Red Hat 6 STIG, Version 1, Release 15

V-38447

Updated finding statement to allow for documented changes due to STIG application.

V-38453

Updated finding statement to allow for documented changes due to STIG application.

V-38454

Updated finding statement to allow for documented changes due to STIG application.

V-38490

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-38514

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-38515

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-38517

Updated the finding statement to only accept “/bin/true” as a valid setting.

V-38593

Adjusted the check to lessen the ambiguity between the “long” and “short” versions of the banner.

V-38667

Adjusted the requirement to support OPORD 16-0080.

V-38682

Updated the finding statement to only accept “/bin/true” as a valid setting.

Solaris 10 SPARC STIG, Version 1, Release 18

V-24357

Corrected Fix instructions to use a semicolon (;) instead of a colon (:) for the plugin definition.

Solaris 10 X86 STIG, Version 1, Release 18

V-24357

Corrected Fix instructions to use a semicolon (;) instead of a colon (:) for the plugin definition.

Solaris 11 SPARC Benchmark, Version 1, Release 6

V-47895

Excluded "solaris-kz" zones from check.

V-48125

Disabled OVAL due to addition of manual steps to STIG.

Solaris 11 SPARC STIG, Version 1, Release 11

V-47895

Added section to Check instructions to identify and exclude any Kernel Zones from the list of local zones.

V-48125

Added exemption to Check instructions for approved and documented users that require access to cron.

V-48213

Corrected Check instructions for the output of the firewall settings and corrected Fix instructions to use the keyword "all".

Solaris 11 X86 Benchmark, Version 1, Release 6

V-47895

Excluded "solaris-kz" zones from check.

V-48125

Disabled OVAL due to addition of manual steps to STIG.

Solaris 11 X86 STIG, Version 1, Release 11

V-47895

Added section to Check instructions to identify and exclude any Kernel Zones from the list of local zones.

V-48125

Added exemption to Check instructions for approved and documented users that require access to cron.

V-48213

Corrected Check instructions for the output of the firewall settings and corrected Fix instructions to use the keyword "all".

SQL Server 2012 Database STIG, Version 1, Release 14

V-41420

System databases cannot be encrypted. Reworded Vulnerability Discussion and Check to make this explicit.

SQL Server 2012 Instance STIG, Version 1, Release 14

V-41044

Added explicit exception for Connect SQL.

Video Services Policy STIG, Version 1, Release 9

Documentation Update

Removed references to VTC STIG.

Video Teleconference STIG, Version 1, Release 7

V-19624

Remove VVoIP/VTC 1740 (V-19624).

V-19658

Remove VVoIP 5705 (V-19658).

V-19659

Remove VVoIP 5710 (V-19659).

V-19660

Remove VVoIP 5715 (V-19660).

V-21514

Remove VVoIP/VTC 1610 (V-21514).

V-21515

Remove VVoIP/VTC 1615 (V-21515).

Voice and Video over Internet Protocol STIG, Version 3, Release 11

V-19445

Remove VVoIP 1510 (V-19672).

V-19446

Remove VVoIP 1515 (V-19672).

V-19626
Remove VVoIP 1730 (V-19626).

V-19627
Move VVoIP 1800 (V-19627) to the Voice Video Services Policy STIG.

V-19633
Remove VVoIP 5525 (V-19633).

V-19651
Move VVoIP 5320 (V-19651) to the Voice Video Services Policy STIG.

V-19652
Move VVoIP 5300 (V-19652) to the Voice Video Services Policy STIG.

V-19653
Remove VVoIP 5305 (V-19653).

V-19654
Move VVoIP 5310 (V-19654) to the Voice Video Services Policy STIG.

V-19655
Remove VVoIP 5315 (V-19655).

V-19656
Remove VVoIP 1600 (V-19656).

V-19657
Remove VVoIP 1605 (V-19657).

V-19658
Remove VVoIP 5705 (V-19658).

V-19659
Remove VVoIP 5710 (V-19659).

V-19660
Remove VVoIP 5715 (V-19660).

V-19661
Modify VVoIP 6200 (V-19661) to reflect NAT is no longer required.

V-19672
Remove VVoIP 6335 (V-19672).

V-21513

Remove VVoIP 1980 (V-21513).

V-21514

Remove VVoIP/VTC 1610 (V-21514).

V-21515

Remove VVoIP/VTC 1615 (V-21515).

V-21516

Move VVoIP 1221 (V-21516) to the Voice Video Services Policy STIG.

V-57951

Move VVoIP 1222 (V-57951) to the Voice Video Services Policy STIG.

V-57953

Move VVoIP 1223 (V-57953) to the Voice Video Services Policy STIG.

Voice Video Endpoint SRG, Version 1, Release 5

V-71671

Modify SRG-NET-000512-VVEP-00065 (V-71671) to correct reference to CNSSI and add reference to JFAN manuals.

Voice Video Services Policy STIG, Version 3, Release 11

V-8328

Modify VVoIP 1005 (V-8328) to reflect NAT is no longer required.

V-19627

Move VVoIP 1800 (V-19627) to the Voice Video Services Policy STIG.

V-19651

Move VVoIP 5320 (V-19651) to the Voice Video Services Policy STIG.

V-19652

Move VVoIP 5300 (V-19652) to the Voice Video Services Policy STIG.

V-19654

Move VVoIP 5310 (V-19654) to the Voice Video Services Policy STIG.

V-21516

Move VVoIP 1221 (V-21516) to the Voice Video Services Policy STIG.

V-57951

Move VVoIP 1222 (V-57951) to the Voice Video Services Policy STIG.

V-57953

Move VVoIP 1223 (V-57953) to the Voice Video Services Policy STIG.

Voice Video Session Management SRG, Version 1, Release 4

V-62105

Modify SRG-NET-000235-VVSM-00046 (V-62105) to correct reference to CNSSI.

V-62117

Modify SRG-NET-000236-VVSM-00047 (V-62117) to correct reference to CNSSI.

V-71689

Modify SRG-NET-000512-VVSM-00057 (V-71689) to correct reference to CNSSI and add reference to JFAN manuals.

Windows 10 Benchmark, Version 1, Release 7

V-63395

Updated the OVAL content to remove tests for file presence and version leaving only the service presence and status tests in conjunction with updates to the manual STIG.

V-63685

Updated the OVAL content to account for different SmartScreen settings in Windows 10 version 1607 in conjunction with modifications to the requirement in the manual STIG.

V-65681

Updated the OVAL content to account for additional Download Mode settings in Windows 10 version 1607 in conjunction with modifications to the requirement in the manual STIG.

V-71769

Updated the OVAL to include a Windows version check.

Benchmark Update

Added new XCCDF profile to disable EMET checks where they are not applicable.

Windows 10 STIG, Version 1, Release 9

V-63319

Changed terminology regarding authentication information protected.

V-63323

Changed terminology regarding authentication information protected.

V-63351

Moved antivirus signature to separate requirement (V-73811).

V-63353
Clarified with regard to EFI partitions.

V-63395
Clarified versions of service being verified.

V-63581
Expanded Vulnerability Discussion on effect of setting.

V-63599
Changed terminology regarding authentication information protected.

V-63603
Updated to note changes in setting in v1607 release.

V-63685
Updated to note changes in setting in v1607 release.

V-63699
Updated to note changes in setting in v1607 release.

V-63701
Updated to note changes in setting in v1607 release.

V-63705
Updated to note changes in setting in v1607 release.

V-63709
Updated to note changes in setting in v1607 release.

V-63713
Updated to note changes in setting in v1607 release.

V-63717
Updated to note changes in setting in v1607 release.

V-63721
Updated to note changes in setting in v1607 release.

V-65681
Updated to note changes in setting in v1607 release.

V-71769
Updated to note setting is applicable starting with v1607 release.

V-73811

Moved antivirus signature to separate requirement (previously part of V-63351). Updated to require configuration of daily checks as well as a maximum age of one week.

Windows 2008 DC Benchmark, Version 6, Release 38

V-8316

Updated the OVAL content to refine the pattern match for NTDS log files.

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2008.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2008.

Windows 2008 DC STIG, Version 6, Release 36

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-8316

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-26683

Updated Check and Fix to align with PKE guidance for mapping accounts.

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.

Windows 2008 MS Benchmark, Version 6, Release 38

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2008.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2008.

Windows 2008 MS STIG, Version 6, Release 36

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.

Windows 2008 R2 DC Benchmark, Version 1, Release 24

V-8316

Updated the OVAL content to refine the pattern match for NTDS log files.

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2008 R2.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2008 R2.

Windows 2008 R2 DC STIG, Version 1, Release 22

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-8316

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-26683

Updated Check and Fix to align with PKE guidance for mapping accounts.

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.

Windows 2008 R2 MS Benchmark, Version 1, Release 25

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2008 R2.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2008 R2.

Windows 2008 R2 MS STIG, Version 1, Release 22

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.

Windows 2012/2012 R2 DC Benchmark, Version 2, Release 8

V-8316

Updated the OVAL content to refine the pattern match for NTDS log files.

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2012.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2012.

V-73805

Created the OVAL to check if the SMB 1.0/CIFS File Sharing Support feature is disabled in Windows 2012 R2.

Windows 2012/2012 R2 DC STIG, Version 2, Release 8

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-8316

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-26683

Updated Check and Fix to align with PKE guidance for mapping accounts.

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 2012/2012 R2 MS Benchmark, Version 2, Release 8

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 2012.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 2012.

V-73805

Created the OVAL to check if the SMB 1.0/CIFS File Sharing Support feature is disabled in Windows 2012 R2.

Windows 2012/2012 R2 MS STIG, Version 2, Release 8

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 7 Benchmark, Version 1, Release 32

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73519

Created the OVAL to check if the SMBv1 protocol for the SMB server is disabled for Windows 7.

V-73523

Created the OVAL to check if the SMBv1 protocol for the SMB client is disabled for Windows 7.

Benchmark Update

Added new XCCDF profile to disable EMET checks where they are not applicable.

Windows 7 STIG, Version 1, Release 26

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.

Windows 8/8.1 Benchmark, Version 1, Release 18

V-15505

Created the OVAL to check if one of the supported versions of the McAfee agents is installed and running.

V-73805

Created the OVAL to check if the SMB 1.0/CIFS File Sharing Support feature is disabled in Windows 8.1.

Benchmark Update

Added new XCCDF profile to disable EMET checks where they are not applicable.

Windows 8/8.1 STIG, Version 1, Release 17

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-36674

Expanded Vulnerability Discussion on effect of setting.

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-73805

Added requirement to disable Server Message Block (SMB) v1.

Windows Firewall Benchmark, Version 1, Release 6

V-17420

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

V-17421

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

V-17430

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

V-17431

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

V-17441

Disabled the rule in OVAL in conjunction with the removal of the requirement from the manual STIG.

Windows Firewall STIG, Version 1, Release 6

V-17420

Removed at DoD Consensus request as providing little benefit.

V-17421

Removed at DoD Consensus request as providing little benefit.

V-17430

Removed at DoD Consensus request as providing little benefit.

V-17431

Removed at DoD Consensus request as providing little benefit.

V-17441

Removed at DoD Consensus request as providing little benefit.

Windows Vista STIG, Version 6, Release 42

V-4107

Raised requirement to CAT I, Windows Vista is no longer supported by Microsoft.

z/OS ACF2 STIG, Version 6, Release 31

V-7482

Updated z/OS Cross Ref of SRRAUDIT spreadsheet to add SDSF as authorized to Start and Stop the SDSF Aux server.

V-17947

Made changes to z/OS Cross Ref of SRRAUDIT spreadsheet to reflect new group for IOA Batch Jobs.

Documentation Update

Update Addendum to add SDSF as authorized to Start and Stop the SDSF Aux server.

Correct typo in addendum. The correct groups are MVREAD - Mainview users that require read only mode and MVUPDT - Mainview users that require some update functions.

Add DASBAUDT to access list for programs DGTFSGDR & DGTFSGLD for ZSMS0012 in Addendum.

Make changes to Addendum to reflect new group for IOA Batch Jobs.

Add description in Addendum clarifying installation datasets.

z/OS BMC CONTROL-M for ACF2 STIG, Version 6, Release 7

V-17947

Reword vulnerability to assure the security of the resources but clarify that the sites have the authority to determine appropriate personnel.

z/OS BMC CONTROL-M for RACF STIG, Version 6, Release 7

V-17947

Reword vulnerability to assure the security of the resources but clarify that the sites have the authority to determine appropriate personnel.

z/OS BMC CONTROL-M for TSS STIG, Version 6, Release 7

V-17947

Reword vulnerability to assure the security of the resources but clarify that the sites have the authority to determine appropriate personnel.

z/OS RACF STIG, Version 6, Release 31

V-7482

Updated z/OS Cross Ref of SRRAUDIT spreadsheet to add SDSF as authorized to Start and Stop the SDSF Aux server.

V-17947

Made changes to z/OS Cross Ref of SRRAUDIT spreadsheet to reflect new group for IOA Batch Jobs.

Documentation Update

Update Addendum to add SDSF as authorized to Start and Stop the SDSF Aux server.

Correct typo in addendum. The correct groups are MVREAD - Mainview users that require read only mode and MVUPDT - Mainview users that require some update functions.

Add DASBAUDT to access list for programs DGTFSGDR & DGTFSGLD for ZSMS0012 in Addendum.

Make changes to Addendum to reflect new group for IOA Batch Jobs.

Add description in Addendum clarifying installation datasets.

Recreate Benchmark

z/OS SRR Scripts, Version 6, Release 31

V-31

Changed scripts to correct error that was documented in ticket.

V-118

Changed scripts to correct error that was documented in ticket.

V-6928

Changed scripts to correct error that was documented in ticket.

V-7482

Changed scripts to correct error that was documented in ticket.

Updated scripts to add SDSF as authorized to Start and Stop the SDSF Aux server.

V-17067

Changed scripts to correct error that was documented in ticket.

V-17947

Changed scripts to correct error that was documented in ticket.

Make changes to scripts to reflect new group for IOA Batch Jobs.

V-17982

Changed scripts to correct error that was documented in ticket.

SRR Script Update

Changes to JCL in CACJ049S to remove RETPD=7.

z/OS TSS STIG, Version 6, Release 31

V-7482

Updated z/OS Cross Ref of SRRAUDIT spreadsheet to add SDSF as authorized to Start and Stop the SDSF Aux server.

V-17947

Made changes to z/OS Cross Ref of SRRAUDIT spreadsheet to reflect new group for IOA Batch Jobs.

Documentation Update

Update Addendum to add SDSF as authorized to Start and Stop the SDSF Aux server.

Correct typo in addendum. The correct groups are MVREAD - Mainview users that require read only mode and MVUPDT - Mainview users that require some update functions.

Add DASBAUDT to access list for programs DGTFSGDR & DGTFSGLD for ZSMS0012 in Addendum.

Make changes to Addendum to reflect new group for IOA Batch Jobs.

Add description in Addendum clarifying installation datasets.

Recreate Benchmark