RED HAT ENTERPRISE LINUX 7 (RHEL7) STIG REVISION HISTORY

Version 3, Release 12

26 July 2023

Developed by DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V3R12	- Red Hat Enterprise Linux 7 STIG, V3R11	- RHEL-07-010199, RHEL-07-010200, RHEL-07-010270 - Corrected "use_authtok" issue. - RHEL-07-020690, RHEL-07-020700, RHEL-07-020710 - Fixed example output. - RHEL-07-031000 - Clarified syslog UDP and VM FDE. - RHEL-07-040300, RHEL-07-040310 - Rule numbers updated due to changes in content management system. - RHEL-07-040320, RHEL-07-040340 - Clarified SSH ClientAliveCountMax wording.	26 July 2023
V3R11	- Red Hat Enterprise Linux 7 STIG, V3R10	- RHEL-07-010019 - Created new rule to ensure vendor GPG keys are installed. - RHEL-07-010063 - Created new rule to disable GNOME login screen user list. - RHEL-07-010119, RHEL-07-010199 - Updated PAM configuration. - RHEL-07-010271 - Revised explanation of emergency account versus temporary account. - RHEL-07-020028 - Created new rule for "mailx". - RHEL-07-020030, RHEL-07-020040 - Updated cron configuration for AIDE.	27 April 2023
V3R10	- Red Hat Enterprise Linux 7 STIG, V3R9	- Rule numbers updated throughout due to changes in content management system. - RHEL-07-010010 - Replaced "egrep" with "grep -E" in check text. - RHEL-07-010060 - Updated check text command GREP syntax. Removed sentence referring to "screen program" from check text. - RHEL-07-010062 - Removed sentence referring to "screen program" from check text. - RHEL-07-010070, RHEL-07-010081, RHEL-07-010082, RHEL-07-010100, RHEL-07-010101, RHEL-07-010110 - Removed sentence referring to "screen program" from check text. Updated formatting in the fix text. - RHEL-07-010090 - Restored required rule that was previously removed without documented reason. - RHEL-07-010100 - Removed sentence referring to "screen program" from check text.	26 January 2023

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Updated formatting in the fix text. Changed GUI to GNOME in check. - RHEL-07-010199 - Created new rule for saving AUTHCONFIG custom settings. - RHEL-07-010200, RHEL-07-010270, RHEL-07-010290, RHEL-07-010320, RHEL-07-010330 - Updated note text to reflect the new AUTHCONFIG rule. - RHEL-07-010342 - Replaced "egrep" with "grep -E" in check text. Updated formatting in the fix text. - RHEL-07-010375 - Created new rule to restrict access to DMESG. - RHEL-07-020029 - Updated check and fix text to include AIDE initialization steps. - RHEL-07-020030, RHEL-07-020040 - Removed lines from check text for checking if AIDE is installed, updated check and fix text to correct mail spool location, and changed IMO to ISSM in vulnerability discussion. - RHEL-07-020650 - Updated check text and formatting in fix. - RHEL-07-021600, RHEL-07-021610, RHEL-07-021620 - Removed lines for checking if AIDE is installed. - RHEL-07-030010 - Updated check text to clarify "failure 1" option use. Updated formatting in the fix text. - RHEL-07-040201, RHEL-07-040610, RHEL-07-040612, RHEL-07-040620, RHEL-07-040630, RHEL-07-040640, RHEL-07-040641, RHEL-07-040650, RHEL-07-040660, RHEL-07-040740, RHEL-07-040830 - Updated check text to include additional SYSCTL directories. Updated formatting in the fix text. - RHEL-07-040420 - Updated requirement to reflect revised SSH key permissions guidance from vendor. - RHEL-07-040470 - Added note specifying to which OS version the rule applies. Updated formatting in the fix text.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- RHEL-07-040611 - Updated check text to include additional SYSCTL directories, updated formatting in the fix text, and updated vulnerability discussion. - RHEL-07-040712 - Created new rule for SSH key exchange algorithms configuration.	
V3R9	- Red Hat Enterprise Linux 7 STIG, V3R8	- RHEL-07-010271 - Added requirement to address emergency accounts. - RHEL-07-010342, RHEL-07-010343, RHEL-07-020023, RHEL-07-030201 - Updated fix text. - RHEL-07-021040, RHEL-07-021700 - Updated check text command to eliminate false positives. - RHEL-07-030840 - Updated check and fix text. - RHEL-07-040160 - Updated check text. - RHEL-07-040310 - Corrected typo in the Vulnerability Discussion. - RHEL-07-040360, RHEL-07-040530 - Updated CCI.	27 October 2022
V3R8	- Red Hat Enterprise Linux 7 STIG, V3R7	- RHEL-07-020029 - Fixed typo in Check text. - RHEL-07-010340, RHEL-07-020230, RHEL-07-030560, RHEL-07-030570, RHEL-07-030580, RHEL-07-030590, RHEL-07-030630, RHEL-07-030640, RHEL-07-030650, RHEL-07-030660, RHEL-07-030670, RHEL-07-030680, RHEL-07-030690, RHEL-07-030710, RHEL-07-030720, RHEL-07-030740, RHEL-07-030750, RHEL-07-030760, RHEL-07-030770, RHEL-07-030780, RHEL-07-030800 RHEL-07-030810, RHEL-07-030819, RHEL-07-030820, RHEL-07-030830 - Updated Check and Fix Text. - RHEL-07-010339, RHEL-07-010342, RHEL-07-010343, RHEL-07-020023 - Updated Check text. - RHEL-07-010483, RHEL-07-010492 - Updated Fix text.	27 July 2022
V3R7	- Red Hat Enterprise	- RHEL-07-010291 - Updated the finding statement in the Check text.	27 April 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	Linux 7 STIG, V3R6		
V3R6	- Red Hat Enterprise Linux 7 STIG, V3R5	- RHEL-07-010190 - Updated check content. - RHEL-07-010290 - Updated rule title. - RHEL-07-010291 - Added requirement to not allow accounts configured with blank or null passwords. - RHEL-07-010310 - Updated discussion, check, and fix content. - RHEL-07-010339 - Added requirement to specify the default "include" directory for the /etc/sudoers file. - RHEL-07-010342, RHEL-07-010343, RHEL-07-020023 - Updated the finding statement. - RHEL-07-010344 - Added requirement to explicitly prevent the bypass of password requirements for privilege escalation. - RHEL-07-020029 - Added requirement for file integrity tool to be installed. - RHEL-07-030370, RHEL-07-030410, RHEL-07-030440, RHEL-07-030510, RHEL-07-030820, RHEL-07-030910 - Grouped like syscalls into this requirement. - RHEL-07-030380, RHEL-07-030390, RHEL-07-030400 - Combined requirement with RHEL-07-030370. - RHEL-07-030420, RHEL-07-030430 - Combined requirement with RHEL-07-030410. - RHEL-07-030450, RHEL-07-030460, RHEL-07-030470, RHEL-07-030480, RHEL-07-030490 - Combined requirement with RHEL-07-030440. - RHEL-07-030500, RHEL-07-030520, RHEL-07-030530, RHEL-07-030540, RHEL-07-030550 - Combined requirement with RHEL-07-030510. - RHEL-07-030821 - Combined requirement with RHEL-07-030820.	27 January 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- RHEL-07-030880, RHEL-07-030890, RHEL-07-030900, RHEL-07-030920 - Combined requirement with RHEL-07-030910. - RHEL-07-040500 - Updated check and fix content.	
V3R5	- Red Hat Enterprise Linux 7 STIG, V3R4	- RHEL-07-010330, RHEL-07-021620, RHEL-07-020020 - Updated check and fix text. - RHEL-07-010343 - Fixed typo in check text. - RHEL-07-010480, RHEL-07-010490 - Removed requirement due to referenced OS version no longer supported by vendor. - RHEL-07-010483, RHEL-07-010492 Updated the discussion and check text with clarifying verbiage. - RHEL-07-010500 - Updated finding statement to include AO approved MFA. - RHEL-07-020021 - Added requirement to confine SELinux users to roles observing least privilege. - RHEL-07-020022 - Added requirement to set SELinux boolean preventing privileged accounts from SSH. - RHEL-07-020023 - Added requirement to configure sudo to elevate SELinux user context. - RHEL-07-020720 - Updated check command syntax. - RHEL-07-040420 - Fixed typos throughout.	27 October 2021
V3R4	- Red Hat Enterprise Linux 7 STIG, V3R3	- RHEL-07-010482 - Updated the requirement to move the superuser requirement for BIOS to a unique STIG ID. - RHEL-07-010483 - Added a requirement to set a unique superuser account for BIOS systems. - RHEL-07-010491 - Updated the requirement to move the superuser requirement for UEFI to a unique STIG ID. - RHEL-07-010492 - Added a requirement to set a unique superuser account for UEFI systems. - RHEL-07-020019 - Updated ESS verbiage throughout the requirement.	23 July 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- RHEL-07-020020, RHEL-07-020210, RHEL-07-020220 - Updated ESS verbiage in the check content. - RHEL-07-020250 - Updated the Vulnerability Discussion and Check content. - RHEL-07-020650 - Updated command in Check content. - RHEL-07-020660 - Updated Rule Title, Vulnerability Discussion, Check, and Fix. - RHEL-07-021030, RHEL-07-021031 - Updated Vulnerability Discussion. - RHEL-07-021100 - Fixed typo in Check and Fix and added a restart daemon statement to the Fix text. - RHEL-07-030330 - Updated the Check and Fix. - RHEL-07-030874 - Fixed typo in Rule Title, Check, and Fix. - RHEL-07-040110, RHEL-07-040400 - Updated statement in Discussion.	
V3R3	- Red Hat Enterprise Linux 7 STIG, V3R2	- RHEL-07-010010 - Updated the command in the Check Content. - RHEL-07-010341 - Added requirement to restrict privilege elevation to authorized personnel. - RHEL-07-010342 - Added requirement to invoke the user's password when using sudo. - RHEL-07-010343 - Added requirement to require re-authentication when using sudo. - RHEL-07-040160 - Updated script syntax. - RHEL-07-040730 - Updated Fix content.	23 April 2021
V3R2	- Red Hat Enterprise Linux 7 STIG, V3R1	- RHEL-07-040110, RHEL-07-040400 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement. - RHEL-07-040710 - Updated Rule Title, Vulnerability Discussion, Check Content, Fix Content to disable X11 Forwarding and downgraded requirement to a CAT II. - RHEL-07-020630 - Updated the command in the Check Content.	22 January 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- RHEL-07-010320 - Updated Fix Text to remove inaccurate information. - RHEL-07-040711 - Added requirement to bind the X11 forwarding server to the loopback address. RHEL-07-020620, RHEL-07-020640, RHEL-07-020650, RHEL-07-020690, RHEL-07-020700, RHEL-07-021000, RHEL-07-021310 - Updated Check Content command.	
V3R1	- Red Hat Enterprise Linux 7 STIG, V2R8	- DISA migrated the Red Hat Enterprise Linux 7 STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V2R8 to V3R1. - RHEL-07-010010 - Fixed typos in the check text command. - RHEL-07-010340 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate". - RHEL-07-020030, RHEL-07-020040 - Updated check text example output. - RHEL-07-020111 - Added not applicable statement to the check text. - RHEL-07-020210, RHEL-07-020220, RHEL-07-030000 - Downgraded to a CAT II. - RHEL-07-021030 - Updated vulnerability discussion, check, and fix to elaborate possible group owners. - RHEL-07-021031 - Added requirement to check that world-writable directories are owned by root, sys, bin, or an application account. - RHEL-07-021340 - Fixed typo in check text finding statement from "and" to "or". - RHEL-07-021350 - Updated check and fix text to verify existence of a key file for FIPS compliance.	23 October 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- RHEL-07-030210, RHEL-07-030211, RHEL-07-030320, RHEL-07-030321 - Updated check text to allow for additional methods of audit log off-load. - RHEL-07-040730 - Generalized overall requirement to cover any graphical display managers. - RHEL-07-910055 - Added requirement to protect audit information.	
V2R8	- Red Hat Enterprise Linux 7 STIG, V2R7	- V-71897 - Removing requirement and combining with RHEL-07-040160. - V-71943 - Updated Check finding statement for "deny" parameter. - V-92255 - Updated Check/Fix to include OPORD 16-0080 verbiage and removed conflicting information. - V-71971 - Updated Check/Fix to include OPORD 16-0080 verbiage, removed conflicting information, and fixed typos. - V-71983 - Removed Not Applicable statement from Check. - V-71989, V-71991 - Updated Check to include OPORD 16-0080 verbiage. Removed Not Applicable statement. - V-71997 - Updated Vulnerability Discussion and Check. - V-72011 - Removed requirement. - V-72015 - Updated Rule Title, Vulnerability Discussion, and Check. - V-81009 - Combined with RHEL-07-021024. - V-81011 - Combined with RHEL-07-021024. - V-81013 - Updated Rule Title, Vulnerability Discussion, Check, and Fix to combine RHEL-07-021022 and RHEL-07-021023. - V-72073 - Updated Vulnerability Discussion to include information about the Advanced Intrusion Detection Environment (AIDE). Removed automatic finding statement from the Check. - V-81015 - Removed requirement and combined with RHEL-07-030201.	24 July 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-81017 - Updated Rule Title, Vulnerability Discussion, and Check. -V-72223 - Updated Rule Title, Vulnerability Discussion, Check, Fix, and CCI. - V-72097, V-72099, V-72101, V-72103, V-72105, V-72107, V-72109, V-72111, V-72113, V-72115, V-72117, V-72119, V-72121, V-72123, V-72125, V-72127, V-72129, V-72131, V-72133, V-72135, V-72137, V-72139, V-72141, V-72149, V-72151, V-72153, V-72155, V-72157, V-72159, V-72161, V-72165, V-72167, V-72171, V-72173, V-72175, V-72177, V-72179, V-72183, V-72185, V-72191, V-72199, V-72201, V-72203, V-72205, V-72207 - Updated Vulnerability Discussion with information about "auid". Updated Check and Fix for "auid!".	
V2R7	- Red Hat Enterprise Linux 7 STIG, V2R6	- V-71861 - Removed references to specific graphic display managers and changed "GUI" to graphical user interface to reduce possible confusion. - V-94843 - Removed references to specific graphic display managers and changed "GUI" to graphical user interface to reduce possible confusion. Added "Not Applicable" statement to the check. Corrected an incorrect file path in the check command. - V-72029 - Updated Check to reference ownership and not group ownership. - V-72417 - Removed "esc" package from the requirement. - V-72225 - Updated check and fix to correct errors in the listed DOD Banner text. - V-72081 - Updated finding statements for clarity. - 100023 - Added a requirement to disable the automount feature in the graphical user interface. - V-72281 - Updated check to verify the /etc/resolv.conf file is "immutable".	24 April 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-71971 - Updated check to allow for organizationally defined roles.	
V2R6	- Red Hat Enterprise Linux 7 STIG, V2R5	- V-71855 - Updated the CCI for this requirement. - V-72269 - Added "chrony" as a valid application that will satisfy the requirement.	24 January 2020
V2R5	- Red Hat Enterprise Linux 7 STIG, V2R4	- V-71899 - Added a "Not Applicable" statement to the requirement. - V-71991 - Updated the second set of commands in the check text. V-71997 - Added End of Life information for RHEL 7.7 to the check. - V-72227, V-72229, V-72231 - Updated the check to look at "id_provider" in the /etc/sssd/sssd.conf file.	25 October 2019
V2R4	- Red Hat Enterprise Linux 7 STIG, V2R3	- V-71855 - Added "--noconfig" to the Check command. - V-71983 - Updated the requirement so that "install usb-storage /bin/true" is defined in a modprobe configuration file. - V-71849 - Updated the check command to include a search for User and Group changes. Updated the fix to properly set the ownership and permissions. - V-71993 - Updated the requirement to be focused on command line disablement of the "Ctrl-Alt-Del" key sequence. - V-71943 - Updated the rule title, added individual finding statements for each required option on the configuration line, and added applicable CCIs to the requirement. - V-72095, V-72097, V-72099, V-72101, V-72103, V-72105, V-72107, V-72109, V-72111, V-72113, V-72115, V-72117, V-72119, V-72121, V-72123, V-72125, V-72127, V-72129, V-72131, V-72133, V-72171, V-72187, V-72189, V-72199, V-72201, V-72203, V-72205, V-72207, V-78999, V-79001 - Updated the requirement to require the definition of both 32- and 64-bit audit rules on a 64-bit system.	26 July 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-72089 - Updated the check and fix to require the "space_left" keyword be set to 25 percent of the total partition size. - V-72217 - Updated the Check and Fix to use the "/etc/security/limits.d/" directory. - V-72029, V-72031, V-72033 – Updated the check and fix commands. - V-72271 - Removed this requirement from the STIG. - V-77821 - Updated the requirement so that "blacklist dccp" was defined in the /etc/modprobe.d/blacklist.conf file. - V-94843 - Added requirement to focus on the disablement of the GUI "Ctrl-Alt-Del" key sequence.	
V2R3	- Red Hat Enterprise Linux 7 STIG, V2R2	- V-81009 - Updated the Check content and Fix text to verify that all /dev/shm entries in /etc/fstab contain nodev. - V81011 - Updated the Check content and Fix text to verify that all /dev/shm entries in /etc/fstab contain nosuid. - V81013 - Updated the Check content and Fix text to verify that all /dev/shm entries in /etc/fstab contain noexec. - V-92251 - Added a requirement that the operating system must use a reverse-path filter for IPv4 traffic on all interfaces. - V-92253 - Added a requirement that the operating system must use a reverse-path filter for IPv4 traffic by default. - V-72065 - Updated the check and fix to allow for static definition of the "/tmp" directory - V-71961 - Updated the initial grep statement in the check content. - V-72275 - Updated the statement in the fix to reference the /etc/pam.d/postlogin file. - V-72149 - Removed the "-F perm=x" from the audit rule - V-72153 - Removed the "-F perm=x" from the audit rule - V-72155 - Removed the "-F perm=x" from the	23 April 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		audit rule - V-72157 - Removed the "-F perm=x" from the audit rule - V-72417 - Removed the "authconfig" and "authconfig-gtk" packages from the requirement. - V-71891 - Updated the grep command to use a wildcard character instead of a specific file name. - V-71897 - Added the "tmux" package as a valid option for compliance. - V-92255 - Added a requirement for the use of a host-based intrusion detection tool - V-71997 - Update the check to include RHEL 7.6 - V-71993 - Update the check to use "ctrl-alt-del.target" instead of "ctrl.alt.del.target"	
V2R2	- Red Hat Enterprise Linux 7 STIG, V2R1	V-71931 - Updated the Check content to produce the correct results. V-71945 - Updated a grammatical mistake in both of the Finding statements. V-71993 - Updated the Fix text to correct a mistake in the "[org/gnome/settings-daemon/plugins/media-keys] logout=" " command. V-72089 - Updated the Finding statement to correct a grammatical error. V-72191 - Updated the Fix text from "insmod" to "kmod". V-72257 - Updated the example output in the Check content and a statement in the Fix text to reflect the proper permission set. V-72269 - Updated the Check content and Fix text so that "maxpoll" is defined on a "server" line.	25 January 2019
V2R1	- NA	- Initial Release.	31 July 2018