SUSE LINUX ENTERPRISE SERVER (SLES) 12 STIG REVISION HISTORY

Version 2, Release 12

25 October 2023

Developed by DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R12	- SLES 12 STIG, V2R11	- SLES-12-010100 - Corrected misspelling in fix. - SLES-12-010340 - Revised check and fix text. - SLES-12-010360 - Removed duplicate requirement.	25 October 2023
V2R11	- SLES 12 STIG, V2R10	- SLES-12-010877 - Revised use of sticky bits.	26 July 2023
V2R10	- SLES 12 STIG, V2R9	- SLES-12-010120 - Corrected typo in check and fix text. - SLES-12-010331 - Created rule to revise explanation of emergency account versus temporary account. - SLES-12-010498 - Created new rule for "mailx". - SLES-12-010500, SLES-12-010510 - Updated cron configuration for AIDE.	27 April 2023
V2R9	- SLES 12 STIG, V2R8	- SLES-12-010375 - Created new rule to restrict access to DMESG. - SLES-12-010499 - Created new rule for AIDE installation and initialization. -SLES-12-010500 - Removed lines from check and fix text for checking if AIDE is installed. Updated check and fix text to correct mail spool location, and updated IMO to ISSM in vulnerability discussion. - SLES-12-010510 - Updated check and fix text to correct mail spool location. - SLES-12-010520, SLES-12-010530 - Removed lines for checking if AIDE is installed. - SLES-12-030220 - Updated rule to reflect revised SSH key permissions guidance from vendor. - SLES-12-030250 - Added note specifying which OS version that the rule applies to. Updated formatting in the fix text. - SLES-12-030270 - Created new rule for SSH key exchange algorithms configuration.	26 January 2023
V2R8	- SLES 12 STIG, V2R7	- SLES-12-010390, SLES-12-030130 - Updated CCI.	27 October 2022
V2R7	- SLES 12 STIG, V2R6	- SLES-12-010109, SLES-12-010113 - Updated Check and Fix text.	27 July 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- SLES-12-010882 - Updated Rule Title, Check, and Fix text. - SLES-12-020490 - Corrected typos in Check and Fix text. - SLES-12-010112 - Updated Check text.	
V2R6	- SLES 12 STIG, V2R5	- SLES-12-010109 - Added requirement to specify the default "include" directory for the /etc/sudoers file. - SLES-12-010112, SLES-12-010113 - Updated the finding statement. - SLES-12-010114 - Added requirement to explicitly prevent the bypass of password requirements for privilege escalation. - SLES-12-010221 - Added requirement to not allow accounts configured with blank or null passwords. - SLES-12-020370, SLES-12-020420, SLES-12-020460, SLES-12-020490, SLES-12-020740 - Grouped like syscalls into this requirement. - SLES-12-020380, SLES-12-020390, SLES-12-020400, SLES-12-020410 - Combined requirement with SLES-12-020370. - SLES-12-020411 - Added a requirement for auditing of unlink, unlinkat, rename, renameat, and rmdir syscalls. - SLES-12-020430, SLES-12-020440, SLES-12-020450 - Combined requirement with SLES-12-020420. - SLES-12-020470, SLES-12-020480 - Combined requirement with SLES-12-020460. - SLES-12-020500, SLES-12-020510, SLES-12-020520, SLES-12-020530, SLES-12-020540 - Combined requirement with SLES-12-020490. - SLES-12-020750 - Combined requirement with SLES-12-020740.	27 January 2022
V2R5	- SLES 12 STIG, V2R4	- SLES-12-010113 - Fixed typo in check text. - SLES-12-010770 - Updated check command syntax.	27 October 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R4	- SLES 12 STIG, V2R3	- SLES-12-010599 - Updated ESS verbiage throughout the requirement. - SLES-12-030170, SLES-12-030180 - Updated statement in Discussion. - SLES-12-030250 - Updated Check and Fix content.	23 July 2021
V2R3	- SLES 12 STIG, V2R2	- SLES-12-010110, SLES-12-010390, SLES-12-010520, SLES-12-010530, SLES-12-030300, SLES-12-030320, SLES-12-030330, SLES-12-030530 - Updated Check content. - SLES-12-010040, SLES-12-010210, SLES-12-010280, SLES-12-010290, SLES-12-010380. SLES-12-010550, SLES-12-010600, SLES-12-010610, SLES-12-010611, SLES-12-010780, SLES-12-010890, SLES-12-010910, SLES-12-020050, SLES-12-020130, SLES-12-030210, SLES-12-030220, SLES-12-030310 - Updated Check and Fix content. - SLES-12-030151 - Updated Rule Title and Vulnerability Discussion. - SLES-12-010113 - Added requirement to require re-authentication when using sudo. - SLES-12-010112 - Added requirement to invoke the user's password when using sudo. - SLES-12-010111 - Added requirement to restrict privilege elevation to authorized personnel - SLES-12-010260, SLES-12-010270 - Updated command syntax and verbiage throughout. - SLES-12-010599 - Updated ESS verbiage throughout the requirement. - SLES-12-010631 - Added requirement to limit account capabilities. - SLES-12-010710 - Updated command syntax. - SLES-12-010871 - Added requirement to set permissions on system library files. - SLES-12-010872 - Added requirement to set permissions on system library directories. - SLES-12-010873 - Added requirement to set the owner of system library files.	23 April 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- SLES-12-010874 - Added requirement to set the owner of system library directories. - SLES-12-010875 - Added requirement to set the group-owner of system library files. - SLES-12-010876 - Added requirement to set the group-owner of system library directories. - SLES-12-010877 - Added requirement to set permissions on system commands. - SLES-12-010878 - Added requirement to set permissions on system command directories. - SLES-12-010879 - Added requirement to set the owner of system commands. - SLES-12-010880 - Removed requirement. - SLES-12-010881 - Added requirement to set the owner of system command directories. - SLES-12-010882 - Added requirement to set the group-owner of system commands. - SLES-12-010883 - Added requirement to set the group-owner of system command directories. - SLES-12-020199 - Updated command syntax and Rule Title typo. - SLES-12-030010 - Removed requirement and combined with SLES-12-030011. - SLES-12-030011 - Added requirement to remove vsftpd package. - SLES-12-030362 - Added requirement to prevent forwarding of IPV6 source-routed packets. - SLES-12-030363 - Added requirement to prevent acceptance of IPV6 ICMP redirect messages. - SLES-12-030364 - Added requirement to prevent IPV6 packet forwarding. - SLES-12-030365 - Added requirement to set default IPV6 packet forwarding behavior	
V2R2	- SLES 12 STIG, V2R1	- SLES-12-030170, SLES-12-030180 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.	22 January 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- SLES-12-030260 - Updated Rule Title, Vulnerability Discussion, Check Content, Fix Content to disable X11Forwarding and downgraded requirement to a CAT II. - SLES-12-030191 - Fixed typos in the Vulnerability Discussion and Check Content. - SLES-12-020250, SLES-12-020260, SLES-12-020280, SLES-12-020310, SLES-12-020320, SLES-12-020550, SLES-12-020560, SLES-12-020570, SLES-12-020580, SLES-12-020600, SLES-12-020610, SLES-12-020620, SLES-12-020630, SLES-12-020640, SLES-12-020670, SLES-12-020680, SLES-12-020690, SLES-12-020700, SLES-12-020710, SLES-12-020720 - Updated auid from 500 to 1000 in Check and Fix Text. - SLES-12-010660 - Removed requirement because it is not a technical control. - SLES-12-030261 - Added requirement to bind the X11 forwarding server to the loopback address. - SLES-12-010710, SLES-12-010730, SLES-12-010740, SLES-12-010750, SLES-12-010790, SLES-12-010850 - Updated Check Content command.	
V2R1	- SLES 12 STIG, V1R6	- DISA migrated the SLES 12 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 V1R6 to V2R1. - SLES-12-010040 - Updated fix text to include command to update the system database as part of the fix. - SLES-12-010070 - Removed incorrect statement referencing a graphical user interface in the check text. - SLES-12-010130 - Updated rule title, vulnerability discussion, check, fix, and CCIs. - SLES-12-010131 - Combined requirement with SLES-12-010130.	23 October 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R6	- SLES 12 STIG, V1R5	- V-92249 - Updated the Parent SRG control and CCI. - V-78003 - This requirement was never published in the SLES 12 STIG. Due to the outdated wording and to minimize confusion we decided to remove this requirement from DPMS and add SLES-12-030611 in its place. - V-102727 - Added a requirement for an anti-virus program to be installed and operating on the system.	24 July 2020
V1R5	- SLES 12 STIG, V1R4	- V-77049, V-77055, V-77057, V-77059, V-77061, V-77065, V-77133 - Removed references to specific graphic display managers and changed "GUI" to graphical user interface to reduce possible confusion. - V-99011 - Downgraded the severity of the requirement from CAT I to CAT II.	24 April 2020
V1R4	- SLES 12 STIG, V1R3	- V-98987 - Added a new requirement for CTRL-ALT-DEL disablement in a Graphical User Interface. - V-99011 - Added a new requirement to check for "PermitUserEnvironment". -V-77051 - Updated the requirement to use /etc/issue. - V-77069 - Updated the requirement to utilize the systemd file structure. - V-77089 - Combined this requirement with V-77105. - V-77105 - Combined V-77089 with this requirement. - V-77117 - Updated the check command to properly identify misconfigured accounts. - V-77123 - Updated the requirement to also include the "retry" value. - V-77131 - Updated the requirement to allow for a delay greater than or equal to 4 seconds. - V-77143, V-77145 - Modified the requirement so that "root" was not the primary account referenced. - V-77149 - Added a note to the requirement that each locally defined partition should be checked.	24 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-77151, V-77153 - Updated the check and fix to better address the actual OS configuration. - V-77155 - Corrected a typo where "xattr" was referenced in the requirement. - V-77171 - Updated the requirement to focus on CLI only. - V-77253 - Added a note to the requirement that each locally defined partition should be checked. - V-77307 - Updated the Rule Title. - V-77327 - Updated the check command to use "grep -iw". V-77329 - Removed the requirement because it is a symlink to "sudo". - V-77333, V-77335 - Corrected a typo in the audit rules. - V-77341 - Removed the requirement. - V-77343, V-77345 - Removed the requirement because it is a symlink to "kmod". - V-77439 - Combined V-77445 with this requirement. - V-77443 - Added "INFO" as a valid configuration option. - V-77445 - Combined this requirement with V-77439. - V-77451 - Removed the "PermitUserEnvironment" from this requirement and added it as a standalone requirement. - V-77469 - Added "sandbox" as a valid configuration option. - V-77471 - Removed "delayed" as a valid configuration option. - V-77509 - Updated a typo in the finding statement. - V-81709 - Updated the requirement to use the "pam_tally2" module.	
V1R3	- SLES 12 STIG, V1R2	- V-77045 - Updated the check content with current version information. - V-77053, V-77055, V-77445 - Updated the requirement to use the correct banner path	25 October 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-77059 - Updated the rule title, check, and fix to reflect that "vloc" is now a part of the "kbd" package. - V-77071, V-81709 - Updated the check and fix to reference the correct location for the desired configuration settings. - V-81785 - Updated the removal action in the fix text to reflect the correct file paths - V-77121 - Corrected the "useauthtok" typo in the check and fix. - V-77137, V-77139 - Updated the command listed in the check. - V-77145 - Updated the file paths in the check and fix. - V-77183, V-77185 - Added a Not Applicable statement to the requirement. - V-77237 - Fixed typo in check text by replacing "nouid" with "nosuid". - V-77293 - Updated the check and fix content to better address the requirement. - V-77297 - Updated the check to verify the root account is assigned to an actual person. Updated the fix to include a command to implement changes to the /etc/aliases file. - V-77301 - Updated the check and fix to ensure that the au-remote plugin was enabled. - V-77311 - Updated the required permissions for /var/log/audit - V-77431 - Updated the check and fix to use the correct configuration "banner_file". - V-77469 - Added a version check and a "Not Applicable" statement to the requirement. - V-77479 - Updated the commands in the Fix Text. - V-77491, V-77493, V-77495 - Updated the commands in the check and fix text. - V-77499 - Updated the command in the check text. - V-77509 - Updated the Vulnerability discussion. Corrected typos in the check and fix text. - V-77311 - Updated the Check and Fix to include "/etc/audit/rules.d/audit.rules".	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-77315, V-77317, V-77319, V-77321, V-77333, V-77335, V-77341, V-77343, V-77345, V-77347, V-77349, V-77351, V-77353, V-77355, V-77357, V-77359, V-77361, V-77363, V-77365, V-77367, V-77369, V-77371, V-77373, V-77375, V-77377, V-77379, V-77381, V-77383, V-77393, V-77405, V-77407, V-77421, V-77423, V-77425, V-77427 - Updated the finding statement to require both 32-bit and 64-bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules". - V-77323 - Updated the Check and Fix to be consistent with other Unix STIGs. - V-77325, V-77327, V-77329, V-77331, V-77337, V-77339, V-77385, V-77387, V-77389, V-77391, V-77395, V-77397, V-77399, V-77401, V-77403, V-77409, V-77411, V-77413, V-77415, V-77417, V-77419 - Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules". - V-97227 - Added a new requirement to remove a default audit rule. - V-77475 - Updated the example output and lowered the maximum allowable value for "maxpoll".	
V1R2	- SLES 12 STIG, V1R1	- V-77169 - Added a Not Applicable statement if HIP or HBSS is installed. - V-102351 - Added a requirement for the use of a host-based intrusion detection tool.	23 April 2019
V1R1	- SLES 12 STIG	- Initial release.	28 September 2018