

UNCLASSIFIED



ORACLE LINUX 7 STIG REVISION HISTORY

Version 2, Release 13

25 October 2023

Developed by Oracle and DISA for the DOD

UNCLASSIFIED

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R13	- Oracle Linux 7 STIG, V2R12	<ul style="list-style-type: none"> - OL07-00-010310 - Revised check and fix text verbiage. - OL07-00-020020 - Revised SELinux guidance. Updated for style guide compliance. - OL07-00-020021 - Revised SELinux guidance. Removed duplicate word from rule title. Updated vuln for style guide compliance. - OL07-00-020023 - Revised SUDO guidance. Updated vuln for style guide compliance. - OL07-00-021700 - Revised verbiage and example output. Updated vuln for style guide compliance. - OL07-00-020230 - Revised SUDO usage. 	25 October 2023
V2R12	- Oracle Linux 7 STIG, V2R11	<ul style="list-style-type: none"> - OL07-00-010199, OL07-00-010200, OL07-00-010270 - Corrected "use_authtok" issue. - OL07-00-020690, OL07-00-020700, OL07-00-020710 - Fixed example output. - OL07-00-031000 - Clarified syslog UDP and VM FDE. - OL07-00-040340 - Clarified SSH ClientAliveCountMax wording. 	26 July 2023
V2R11	- Oracle Linux 7 STIG, V2R10	<ul style="list-style-type: none"> - OL07-00-010019 - Created new rule to ensure vendor GPG keys are installed. - OL07-00-010063 - Created new rule to disable GNOME login screen user list. - OL07-00-010119, OL07-00-010199 - Updated PAM configuration. - OL07-00-010271 - Revised explanation of emergency account versus temporary account. - OL07-00-020028 - Created new rule for "mailx". - OL07-00-020030, OL07-00-020040 - Updated cron configuration for AIDE. 	27 April 2023
V2R10	- Oracle Linux 7 STIG, V2R9	<ul style="list-style-type: none"> - Rule numbers updated throughout due to changes in content management system. - OL07-00-010010, OL07-00-010342 - Replaced "egrep" with "grep -E" in check text. Updated formatting in the fix text. - OL07-00-010060, OL07-00-010062, OL07-00-010070, OL07-00-010081, OL07-00-010082, OL07-00-010100, OL07-00-010101, 	26 January 2023

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>OL07-00-010110 - Removed sentence referring to "screen program" from check text. Updated formatting in the fix text.</p> <ul style="list-style-type: none"> - OL07-00-010090 - Restored required rule that was previously removed without documented reason. - OL07-00-010199 - Created new rule for saving AUTHCONFIG custom settings. - OL07-00-010200, OL07-00-010270, OL07-00-010290 - Updated note text to reflect the new AUTHCONFIG rule. OL07-00-010320, OL07-00-010330 - Updated note text to reflect the new AUTHCONFIG rule; fixed typo in check. - OL07-00-010375 - Created new rule to restrict access to DMESG. - OL07-00-020029 - Updated check and fix text to include AIDE initialization steps. - OL07-00-020030, OL07-00-020040 - Removed lines from check text for checking if AIDE is installed, updated fix text to correct mail spool location, and updated IMO to ISSM in vulnerability discussion. - OL07-00-020650 - Replaced smart quotes in check text. Updated formatting in the fix text. - OL07-00-021600, OL07-00-021610, OL07-00-021620 - Removed lines for checking if AIDE is installed. - OL07-00-030010 - Updated check text to clarify "failure 1" option use. Updated formatting in the fix text. - OL07-00-040201, OL07-00-040510, OL07-00-040610, OL07-00-040612, OL07-00-040620, OL07-00-040630, OL07-00-040640, OL07-00-040641, OL07-00-040650, OL07-00-040660, OL07-00-040740, OL07-00-040830 - Updated check text to include additional SYSCTL directories. - OL07-00-040420 - Updated text to reflect revised SSH key permissions guidance from vendor. Updated formatting in the fix text. - OL07-00-040470 - 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
		<ul style="list-style-type: none"> - OL07-00-040611 - Updated check text to include additional SYSCTL directories, updated formatting in the fix text, and updated vulnerability discussion. - OL07-00-040712 - Created new rule for SSH key exchange algorithms configuration. 	
V2R9	- Oracle Linux 7 STIG, V2R8	<ul style="list-style-type: none"> - OL07-00-010271 - Added requirement to address emergency accounts. - OL07-00-010342, OL07-00-020023, OL07-00-030201 - Updated fix text. OL07-00-010343, OL07-00-030840 - Updated check and fix text. - OL07-00-021040, OL07-00-021700 - Updated check text command to eliminate false positives. - OL07-00-040160 - Updated check text. - OL07-00-040310 - Corrected typo in the Vulnerability Discussion. - OL07-00-040360, OL07-00-040530 - Updated CCI. 	27 October 2022
V2R8	- Oracle Linux 7 STIG, V2R7	<ul style="list-style-type: none"> - OL07-00-010010 - Fixed typo in Check command. - OL07-00-010340, OL07-00-020230, OL07-00-030560, OL07-00-030570, OL07-00-030580, OL07-00-030590, OL07-00-030630, OL07-00-030640, OL07-00-030650, OL07-00-030660, OL07-00-030670, OL07-00-030680, OL07-00-030690, OL07-00-030710, OL07-00-030720, OL07-00-030740, OL07-00-030750, OL07-00-030760, OL07-00-030770, OL07-00-030780, OL07-00-030800, OL07-00-030810, OL07-00-030819, OL07-00-030820, OL07-00-030830 - Updated Check and Fix text. - OL07-00-010339, OL07-00-010342, OL07-00-010343, OL07-00-020023 - Updated Check text. - OL07-00-010483, OL07-00-010492 - Updated Fix text. - OL07-00-020029 - Fixed typo in Check text. 	27 July 2022
V2R7	- Oracle Linux 7 STIG, V2R6	<ul style="list-style-type: none"> - OL07-00-010500 - Updated the finding statement in the Check text. 	27 April 2022

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R6	- Oracle Linux 7 STIG, V2R5	<ul style="list-style-type: none"> - OL07-00-010190 - Updated check content. - OL07-00-010290 - Updated rule title. - OL07-00-010291 - Added requirement to not allow accounts configured with blank or null passwords. - OL07-00-010310 - Updated discussion, check, and fix content. - OL07-00-010339 - Added requirement to specify the default "include" directory for the /etc/sudoers file. - OL07-00-010342, OL07-00-010343, OL07-00-020023 - Updated the finding statement. - OL07-00-010344 - Added requirement to explicitly prevent the bypass of password requirements for privilege escalation. - OL07-00-020029 - Added requirement for file integrity tool to be installed. - OL07-00-030380, OL07-00-030390, OL07-00-030400 - Combined requirement with OL07-00-030370. - OL07-00-030370, OL07-00-030410, OL07-00-030440, OL07-00-030510, OL07-00-030820, OL07-00-030910 - Grouped like syscalls into this requirement. - OL07-00-030420, OL07-00-030430 - Combined requirement with OL07-00-030410. - OL07-00-030450, OL07-00-030460, OL07-00-030470, OL07-00-030480, OL07-00-030490 - Combined requirement with OL07-00-030440. - OL07-00-030500, OL07-00-030520, OL07-00-030530, OL07-00-030540, OL07-00-030550 - Combined requirement with OL07-00-030510. - OL07-00-030821 - Combined requirement with OL07-00-030820. - OL07-00-030880, OL07-00-030890, OL07-00-030900, OL07-00-030920 - Combined requirement with OL07-00-030910. - OL07-00-040500 - Updated check and fix content. 	27 January 2022

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R5	- Oracle Linux 7 STIG, V2R4	<ul style="list-style-type: none"> - OL07-00-010330, OL07-00-020020, OL07-00-021620 - Updated check and fix text. - OL07-00-010343- Fixed typo in check text. - OL07-00-010480, OL07-00-010490 - Removed requirement due to referenced OS version no longer supported by vendor. - OL07-00-010483, OL07-00-010492 - Updated the discussion and check text with clarifying verbiage. - OL07-00-010500 - Updated finding statement to include AO approved MFA. - OL07-00-020021 - Added requirement to confine SELinux users to roles observing least privilege. - OL07-00-020022 - Added requirement to set SELinux boolean preventing privileged accounts from SSH. - OL07-00-020023 - Added requirement to configure sudo to elevate SELinux user context. - OL07-00-020720 - Updated check command syntax. - OL07-00-040420 - Fixed typos throughout. 	27 October 2021
V2R4	- Oracle Linux 7 STIG, V2R3	<ul style="list-style-type: none"> - OL07-00-010482 - Updated the requirement to move the superuser requirement for BIOS to a unique STIG ID. - OL07-00-010483 - Added a requirement to set a unique superuser account for BIOS systems. - OL07-00-010491 - Updated the requirement to move the superuser requirement for UEFI to a unique STIG ID. - OL07-00-010492 - Added a requirement to set a unique superuser account for UEFI systems. - OL07-00-020019 - Updated ESS verbiage throughout the requirement. - OL07-00-020020, OL07-00-020210 OL07-00-020220 - Updated ESS verbiage in the Check content. - OL07-00-020650 - Updated command in Check content. 	23 July 2021

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - OL07-00-020660 - Updated Rule Title, Vulnerability Discussion, Check, and Fix. - OL07-00-021030, OL07-00-021031 - Updated Vulnerability Discussion. - OL07-00-021100 - Fixed typo in Check and Fix and added a restart daemon statement to the Fix text. - OL07-00-030330 - Updated the Check and Fix. - OL07-00-030874 - Fixed typo in Rule Title, Check, and Fix. - OL07-00-040110, OL07-00-040400 - Updated statement in Discussion. 	
V2R3	- Oracle Linux 7 STIG, V2R2	<ul style="list-style-type: none"> - OL07-00-010010 - Updated the command in the check content and spacing in the fix text. - OL07-00-010343 - Added requirement to require re-authentication when using sudo. - OL07-00-010342 - Added requirement to invoke the user's password when using sudo. - OL07-00-010341 - Added requirement to restrict privilege elevation to authorized personnel. - OL07-00-040160 - Updated time designation and script syntax. - OL07-00-040730 - Updated Fix content. 	23 April 2021
V2R2	- Oracle Linux 7 STIG, V2R1	<ul style="list-style-type: none"> - OL07-00-040480 - Removed requirement as DNSSEC is better handled thru a DNS-centric STIG. (e.g., BIND STIG) - OL07-00-040110, OL07-00-040400 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement. - OL07-00-040710 - Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Content to disable X11Forwarding and downgraded requirement to a CAT II. - OL07-00-010320 - Updated Fix Text to remove inaccurate information. - OL07-00-040711 - Added requirement to bind the X11 forwarding server to the loopback address. 	22 January 2021

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- OL07-00-020630, OL07-00-020620, OL07-00-020640, OL07-00-020650, OL07-00-020690, OL07-00-020700, OL07-00-021000, OL07-00-021310 - Updated Check Content command.	
V2R1	- Oracle Linux 7 STIG, V1R2	<p>- DISA migrated the Oracle 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 V1R2 to V2R1.</p> <p>- OL07-00-010010 - Updated check, fix, and CCI's.</p> <p>- OL07-00-010020 - Updated check text and CCI's.</p> <p>- OL07-00-010040 - Removed specific references to GNOME and replaced with Graphical User Interface.</p> <p>- OL07-00-010100 - Added not applicable statement to the check text.</p> <p>- OL07-00-010320 - Updated rule title, check text, and CCI's.</p> <p>- OL07-00-010340 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate".</p> <p>- OL07-00-010350 - Added requirement for users to re-authenticate for privilege escalation.</p> <p>- OL07-00-020020 - Updated check, fix, and CCI's.</p> <p>- OL07-00-020030 - Updated check text example output.</p> <p>- OL07-00-020040 - Updated check text example output and upgraded severity to a CAT II.</p> <p>- OL07-00-020100 - Updated check, fix, and CCI's.</p> <p>- OL07-00-020101 - Updated check text to include verification that the DCCP kernel module is disabled.</p>	23 October 2020

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - OL07-00-020111 - Added new requirement to check the graphical user interface automounter is disabled. - OL07-00-020210 - Downgraded to a CAT II and added verbiage to the check text. - OL07-00-020220 - Added requirement for SELinux targeted policy. - OL07-00-010090, OL07-00-010219, OL07-00-020600, OL07-00-030200 - Removed requirement. - OL07-00-020230 - Removed references to GNOME. - OL07-00-020231- Added requirement to disable Ctrl-Alt-Delete key sequence for the Graphical User Interface. - OL07-00-020620 - Updated rule title, vulnerability discussion, and check text. - OL07-00-020690, OL07-00-040170 - Updated check and fix text. - OL07-00-020700, OL07-00-020710 - Updated commands in check and fix text. - OL07-00-021024 - Updated requirement to combine OL07-00-021022 and OL07-00-021023. - OL07-00-021030 - Updated vulnerability discussion, check, and fix text to elaborate on possible group owners. - OL07-00-021031 - Added new requirement to check that world-writable directories are owned by root, sys, bin, or an application account. - OL07-00-021340 - Fixed typo in check text finding statement from "and" to "or". - OL07-00-021350 - Updated check and fix text to verify existence of a key file for FIPS compliance. - OL07-00-021620 - Updated vulnerability discussion and check text. - OL07-00-030000 - Downgraded to a CAT II. - OL07-00-030010 - Updated check text and CCI's. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - OL07-00-021022, OL07-00-021023 - Combined requirement with OL07-00-021024. - OL07-00-030201 - Updated rule title, vulnerability discussion, and check text to allow for alternative methods of off-loading audit logs. - OL07-00-030210, OL07-00-030211 - Updated check text to allow for additional methods of audit log off-load. - OL07-00-030320, OL07-00-030321 - Updated check text to allow for additional methods of audit log off-load. OL07-00-030330 - Fixed typo in check and fix text. - OL07-00-030370, OL07-00-030380, OL07-00-030390, OL07-00-030400 - Updated vulnerability discussion, check text, fix text, and CCIs. - OL07-00-030360, OL07-00-030410, OL07-00-030420, OL07-00-030430, OL07-00-030440, OL07-00-030450, OL07-00-030460, OL07-00-030470, OL07-00-030480, OL07-00-030490, OL07-00-030500, OL07-00-030510, OL07-00-030520, OL07-00-030530, OL07-00-030540, OL07-00-030550 - Updated vulnerability discussion, check, and fix text. - OL07-00-030740, OL07-00-030819, OL07-00-030821, OL07-00-030880, OL07-00-030890, OL07-00-030900, OL07-00-030910, OL07-00-030920 - Updated check and fix text to include both 32-bit and 64-bit architectures. - OL07-00-040000 - Updated check and fix text to include additional directory for setting maxlogins. -OL07-00-040180, OL07-00-040190, OL07-00-040200 - Updated check text with a not applicable statement. - OL07-00-040500 - Updated check and fix text to include additional ntp service. OL07-00-040600 - Updated rule title and check text. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - OL07-00-040730 - Generalized overall requirement to cover any graphical display managers. - OL07-00-041001 - Updated vulnerability discussion, check, fix, and CCIs. 	
V1R2	- Oracle Linux 7 STIG, V1R1	<ul style="list-style-type: none"> - V-99165, V-99539 - Updated Group ID. - V-99295, V-99297, V-99299, V-99301, V-99303, V-99305, V-99307, V-99309, V-99311, V-99313, V-99315, V-99317, V-99319, V-99321, V-99323, V-99325, V-99327, V-99329, V-99331, V-99333, V-99335, V-99337, V-99339, V-99345, V-99347, V-99349, V-99351, V-99353, V-99355, V-99357, V-99361, V-99363, V-99365, V-99367, V-99369, V-99371, V-99373, V-99375, V-99377, V-99387, V-99399, V-99401, V-99403, V-99405, V-99407 - Updated Vulnerability Discussion with information about "audit". Updated the Check Content and Fix Text for "audit". 	24 July 2020
V1R1	- NA	- Initial Release.	03 February 2020