IBM AIX 7.x STIG
REVISION HISTORY

Version 2, Release 7

27 April 2023

Developed by IBM and DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R7	- IBM AIX 7.x STIG, V2R6	- AIX7-00-001024 - Removed requirement for deprecated OpenSSH option "printlastlog". - Rule keys updated throughout due to changes in content management system.	27 April 2023
V2R6	- IBM AIX 7.x STIG, V2R5	- AIX7-00-002147, AIX7-00-002148, AIX7-00-002150 - Updated Rule Title, Check, and Fix text.	27 July 2022
V2R5	- IBM AIX 7.x STIG, V2R4	- AIX7-00-002140, AIX7-00-002144 - Updated the command output in the check text to reflect system group. - AIX7-00-002141, AIX7-00-002145 - Updated Title, Check, and Fix content to reflect system group. - AIX7-00-002142, AIX7-00-002146 - Updated Check and Fix to reflect system group.	27 April 2022
V2R4	- IBM AIX 7.x STIG, V2R3	- AIX7-00-001032 - Updated check commands to search "/root" instead of "/home/root". - AIX7-00-001130 - Updated the example text in the check to reflect the correct value for "default minspecialchar" to 1. - AIX7-00-003062 - Added a Not Applicable statement to the requirement for systems utilizing IPv6.	27 January 2022
V2R3	- IBM AIX 7.x STIG, V2R2	- AIX7-00-002038 - Corrected "UTC" typos in the check and fix content. - AIX7-00-002077 - Updated the rule to only check for ownership of the /etc/inetd.conf file. - AIX7-00-002092 - Added a requirement for the /etc/inetd.conf file to be group-owned by "system". - AIX7-00-002093 - Added a requirement for /etc/inetd.conf to have a permission set of 0640 or less permissive. - AIX7-00-002125 - Removed requirement; the parent SRG requirement has been removed from the SRG. - AIX7-00-002140 - Added a requirement for /etc/hosts to be owned by "root".	23 July 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- AIX7-00-002141 - Added a requirement for /etc/hosts to be group-owned by "root". - AIX7-00-002142 - Added a requirement for /etc/hosts to have a permission set of 0640 or less permissive. - AIX7-00-002143 - Added a requirement for cron and crontab directories to have a permission set of 0640 or less permissive. - AIX7-00-002144 - Added a requirement for /etc/syslog.conf to be owned by "root". - AIX7-00-002145 - Added a requirement for /etc/syslog.conf to be group-owned by "root". - AIX7-00-002146 - Added a requirement for /etc/syslog.conf to have a permission set of 0640 or less permissive. - AIX7-00-002147 - Added a requirement that the /var/spool/cron/atjobs directory must be owned by "daemon". - AIX7-00-002148 - Added a requirement that the /var/spool/cron/atjobs directory must be group-owned by "daemon". - AIX7-00-002149 - Added a requirement for the /var/spool/cron/atjobs directory to have a permission set of 0640 or less permissive. - AIX7-00-002150 - Added a requirement for the cron and crontab directories to be group-owned by "cron".	
V2R2	- IBM AIX 7.x STIG, V2R1	- AIX7-00-002105 - Updated "ClientAliveInterval" value to "600". Combined this requirement with AIX7-00-003002. - AIX7-00-003002 - Combined requirement with AIX7-00-002105.	23 April 2021
V2R1	- IBM AIX 7.x STIG, V1R2	- DISA migrated the IBM AIX 7.x 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.	23 October 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- AIX7-00-001025 - Updated an incorrect file path in the check content. - AIX7-00-002070 - Updated the requirement to allow for file ownership by a system account. - AIX7-00-002071 - Updated the requirement to allow for file group ownership by a system group. - AIX7-00-003143 - Updated the parent SRG ID assigned to this requirement.	
V1R2	- IBM AIX 7.x STIG, V1R1	- V-91775 - Updated the check so that it is only looking at the "/etc/security/audit/objects" file. - V-100005 - Added a requirement to address actions when the audit storage volume is full. - V-91341 - Corrected a typo in the rule title and vulnerability discussion.	24 April 2020
V1R1	- N/A	- Initial Release.	25 April 2019