Product Support Notice

PSN # PSN005048u

Original publication date: 7-Aug-2017. This is Issue #21, published date: 26-Jul-2022.

Severity/ risk level: High

Urgency: When convenient

Name of problem

Security Updates - Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2.0.

Products affected

Avaya Aura® Experience Portal 7.2.0

Known Issues

A previous version of this patch, that is “1707”, including a Red Hat-supplied kernel that caused a Java issue.

When upgrading to kernel with the fix for stack guard flaw, a crash could occur in Java Virtual Machine (JVM) environments, which attempted to implement their own stack guard page. With this update, the underlying source code has been fixed to consider the PROT_NONE mapping as a part of the stack, and the crash in JVM no longer occurs under the described circumstances. (BZ#1466667)

Problem description

Avaya periodically issues security update hotfixes for the version of Linux shipped with bundled and OVA-based Experience Portal systems. These hotfixes address security vulnerabilities in Avaya Enterprise Linux.

Resolution

Periodically download the latest Avaya Enterprise Linux security updates hotfix and install it on each server in your Experience Portal system.

Additional configuration changes customers can do to improve their system security:

These changes are not automated as part of the patch; they must be done by a system administrator.

SSH Sever Public Key is too small	Do not load Server keys under 2048 bits It is now recommended that server keys under 2048 not be used. Define the valid keys to load. # sed -i '/ssh_host_rsa_key/ s/^#//' /etc/ssh/sshd_config # /etc/init.d/sshd restart
Deprecated SSH Cryptographic Settings	KexAlgorithms default is used, and it includes now deprecated sha1, so define and only specify sha256 based algorithm. # echo "KexAlgorithms diffie-hellman-group-exchange-sha256" >> /etc/ssh/ssh_config # echo "KexAlgorithms diffie-hellman-group-exchange-sha256" >> /etc/ssh/sshd_config # /etc/init.d/sshd restart

CVE-2020-1938: Ghostcat - Apache Tomcat AJP File Read/Inclusion Vulnerability	The Main and MMS Tomcat of AEP have the AJP port limited to localhost by default, this restricts remote exploitation.
	If the customer has implemented the optional applications server included with the product, they should make the following change:
	• Modify the server.xml file
	  ○ vi $APPSERVER_HOME/conf/server.xml
	• find ‘<Connector port="7009"’
	• Make line look like:
	  ○ <Connector port="7009" protocol="AJP/1.3" secretRequired="false" address="127.0.0.1" redirectPort="7443" />
	  ▪ You will have to add the green part.
	• Then save the file.
	• Restart the application Tomcat
	  ○ /etc/init.d/appserver restart
	This will limit access to AJP to the local system, not a remote attacker.

Workaround or alternative remediation

n/a

Remarks

Software-only customers will need to obtain Linux security updates directly from Red Hat, they can see the Readme referenced (RELATED DOCUMENTS) on the Downloads page below for the “PACKAGES UPDATED” section, This is a list of the updated packages tested by Avaya with the AAEP product.

Patch Notes

The information in this section contains the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Downloads:

https://support.avaya.com/downloads/download-details.action?contentId=C2017831743556470_7&productId=P0407&releaseId=7.2.x

Patch install instructions	Service-interrupting?
See the `readme.txt` that is bundled with the hotfix. 1. To complete the patching process, reboot each server after patches are installed. 2. A properly configured multi-server system with primary and secondary EPM and multiple MPP can be patched without total service interruption.	Yes

Verification

See the readme.txt that is bundled with the hotfix.

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

See the readme.txt that is bundled with the hotfix.

Avaya Security Vulnerability Classification

High

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.