



Product Support Notice

© 2021 Avaya Inc. All Rights Reserved.

PSN # PSN004791u

Original publication date: 01-Aug-2016. This is Issue #23, published date: 21-Oct-2021. Severity/risk level: High Urgency: When convenient

Name of problem

Security Updates - Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.1.0.

Products affected

Avaya Aura® Experience Portal 7.1.0

Note: This is the final patch for Experience Portal 7.1.0. Customers are encouraged to move to Experience Portal 8.x to continue to receive security patches.

Known Issues

A previous version of this patch, that is, "1707" included 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, and the system should be rebooted after applying them.

Close cups port 631	<p>Port 631 is open and it does not need to be. There is no real service listening on the port. The cups package sets up the portreserve application which binds port 631 to an external interface.</p> <pre># chkconfig grep portreserve portreserve 0:off 1:off 2:on 3:on 4:on 5:on 6:off</pre> <pre># ls -la /etc/portreserve/ -rw-r--r-- 1 sroot root 4 Jun 10 2015 cups</pre> <pre># netstat -annp grep 631 udp 0 0 0.0.0.0:631 0.0.0.0:* 1629/portreserve</pre> <p>Run the following commands to close the port and prevent it from opening upon reboot:</p> <pre># portrelease cups # rm -rf /etc/portreserve/cups</pre>
Configure Network Time Protocol (NTP) - restrict default	<p>Restrict the defaults of NTP for Security</p> <pre># echo "restrict default kod nomodify notrap nopeer noquery" >>/etc/ntp.conf # echo "restrict -6 default kod nomodify notrap nopeer noquery" >>/etc/ntp.conf # service ntpd restart</pre>
SSH Weak Algorithms	<p>Restrict ssh from using weak algorithms.</p> <pre># vi /etc/ssh/sshd_config (Find and set the Ciphers to match) Ciphers aes256-ctr,aes192-ctr,aes128-ctr # service sshd restart</pre>

SSH Sever Public Key too small	<p>Do not load Server keys under 2048 bits</p> <p>It is now recommended that server keys under 2048 not be used.</p> <p>Define the valid keys to load.</p> <pre># sed -i '/ssh_host_rsa_key/ s/^#//' /etc/ssh/sshd_config # /etc/init.d/sshd restart</pre>
Deprecated SSH Cryptographic Settings	<p>KexAlgorithms default is used, and it includes now deprecated sha1, so define and only specify sha256 based algorithm.</p> <pre># 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</pre>
CVE-2020-1938: Ghostcat - Apache Tomcat AJP File Read/Inclusion Vulnerability	<p>The Main and MMS Tomcat of AEP have the AJP port limited to localhost by default, this restricts remote exploitation.</p> <p>If the customer has implemented the optional applications server included with the product, they should make the following change:</p> <ul style="list-style-type: none"> • Modify the server.xml file <ul style="list-style-type: none"> ○ vi \$APPSERVER_HOME/conf/server.xml • find '<Connector port="7009"' • Make line look like: <ul style="list-style-type: none"> ○ <Connector port="7009" protocol="AJP/1.3" secretRequired="false" address="127.0.0.1" redirectPort="7443" /> <ul style="list-style-type: none"> ▪ You will have to add the green part. • Then save file. • Restart the application Tomcat <ul style="list-style-type: none"> ○ /etc/init.d/appserver restart <p>This will limit access to AJP to the local system, not a remote attacker.</p>

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 concerns 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=C2016428115413600_9&productId=P0407&releaseId=7.1.x

Patch install instructions

Service-interrupting?

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

Yes

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.

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](#).

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners.