Product Support Notice

PSN #	PSN005774u				
Original publication date: 26-Jan-2021. This is Issue #08, published date: 2-Dec-2022.		Severity/risk level	High	Urgency	When convenient

Name of problem

Security Updates - Avaya Enterprise Linux for Avaya Experience Portal 8.x.

Products affected

Avaya Experience Portal 8.0
Avaya Experience Portal 8.1
Avaya Experience Portal 8.1.1
Avaya Experience Portal 8.1.2

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.

Workaround or alternative remediation

- As of AVL patch 2021-07, AEP 8.0 systems configured for FIPS must be at EPM patch 8.0.0.0.1473 or later due to changes in the Java 1.8.0 delivered with this package.
  Failure to be at the needed patch level will result in java exceptions at the end of the AVL patch process.
  Exception in thread "main" java.security.ProviderException: Crypto provider not installed: BCFIPS SunPKCS11-NSS-FIPS
  If this occurs simply apply EPM patch 8.0.0.0.1473+ and the system will function again.
  **Note: AVL patches before 2021-10 installation broke the EASG prompt on SSH logins, this is now addressed in the AVL patch. To restore the EASG prompt on older AVL patches do the following (Not needed for systems on AVL patches on or after 2021-10):
  1) rm /etc/pam.d/system-auth
  2) ln -s /etc/pam.d/system-auth-AAEP /etc/pam.d/system-auth
- The AVL patch will improve system security, this may have implications for the certificate used on the WebLM component. It is recommended that the user reference this KB SOLN356009 to update to a 2048-bit certificate to allow connection after the system security is tightened.
  1) If the WebLM certificate was not updated and the AVL 2021-10 patch was applied, it could impact getting licenses.
  2) To fix:
     a. As a user with root permissions on the PRI EPM system.
     b. update-crypto-policies –show
        i. This should show “LEGACY”
     c. If it does not execute:
        i. update-crypto-policies –set LEGACY
- As of AVL patch 2021-10 additional security strengthening was implemented, this includes tighter password rules and account aging and lockout to have the system be more in compliance with heightened security such as Payment Card Industry (PCI) compliance. See the Readme.txt that is bundled with the hotfix for more information.

Remarks

Software-only customers will need to obtain Linux security updates directly from Red Hat, they can see the Readme.txt 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.

Software Images

Software Images	PLDS ID	Target Customer Base
epavl-8.x.x.0.2210.tar.gz epavl-8.x.x.0.2210.sha256.sig	AEP00000129 AEP00000130	(Bundled customers)
8.0.0.0.1517.tar.gz 8.0.0.0.1517.tar.gz.sig	AEP00000109 AEP00000110	(MPP Patch – All customers)
EPM_8.0.0.0.1517.tar.gz	AEP00000111	(EPM Patch – All customers)
8.1.1.0.0261.tar.gz 8.1.1.0.0261.tar.gz.sig	AEP00000112 AEP00000113	(MPP Patch – All customers)
EPM_8.1.1.0.0261.tar.gz	AEP00000114	(EPM Patch – All customers)
8.1.2.0.0328.tar.gz 8.1.2.0.0328.tar.gz.sig	AEP00000126 AEP00000127	(MPP Patch – All customers)
EPM_8.1.1.0.0328.tar.gz	AEP00000128	(EPM Patch – All customers)

Patch Notes

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

Backup before applying the patch

n/a

Download

https://support.avaya.com/downloads/download-details.action?contentId=C2021112154544200_8

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 the patches are installed.
2. A properly configured multi-server system with primary and secondary EPM and multiple MPPs 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.