Product Support Notice

PSN # PSN020539u

Original publication date: 25-Oct-21. This is Issue #01, published date: 25-Oct-21.

Severity/risk level: High | Urgency: Immediately

Name of problem

PSN020539u - Avaya Aura® Application Enablement (AE) Services 10.1 Client and SDK Information

Products affected

Avaya Aura® Application Enablement (AE) Services, 7.x, 8.x, 10.1 (future release)

Problem description

This PSN is for informational and future planning purposes only.

Avaya Aura® Release 10.1 is targeted for release in December 2021.

AE Services 10.1 will run on RHEL 8 and this required third party libraries to be updated when creating TSAPI and CVLAN 10.1 clients and SDKs for AE Services 10.1.

AE Services 10.1 TSAPI and CVLAN Clients and SDKs will only be supported on RHEL 8.

Resolution

Note: Avaya recommends that AE Services and Clients always be on the same version.

The following Client/Server Release combinations will be supported.

AES SERVER RELEASE	SUPPORTED TSAPI & CVLAN CLIENT RELEASE
AES 10.1	**8.1.x RHEL 7** **8.0.x RHEL 7** **10.1 RHEL 8**
AES 8.1.3	**8.1.x RHEL 7** **8.0.x RHEL 7** **10.1 RHEL 8**

Table 1: Supported Server and Client Release Combinations

Note: TSAPI Client, SDK and CVLAN client versions 8.1.x RHEL 6 and 8.0.x RHEL 6 are only supported during a transient period while upgrading the AE Services. Bug fixes from Red Hat will no longer be available for RHEL 6. Once AE Services is running release 10.1, TSAPI and CVLAN clients must be upgraded per Table 1 above.

Workaround or alternative remediation

NA

Remarks

Issue 1 – Oct 25, 2021.

Patch Notes

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

Backup before applying the patch

Always.

Download

NA

Patch install instructions | **Service-interrupting?**

NA | Yes

Verification
NA
Failure
NA.
Patch uninstall instructions
NA

Security Notes

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

Security risks
N/A
Avaya Security Vulnerability Classification
N/A
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.