Product Support Notice

PSN #	PSN020444u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 16-Dec-19. This is Issue #04, published date: 12-Feb-20.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN020444u – Major browsers deprecating Transport Layer Security (TLS) 1.0 and 1.1 in March 2020

Products affected

All Avaya applications with a Web User Interface (UI) running on operating system versions which cannot support TLS 1.2, including:

- Avaya Aura® Communication Manager (CM) 6.3.x and earlier
- Avaya Aura® Application Enablement Services (AES) 7.0 and earlier
- Avaya Aura® System Manager (SMGR) & WebLM 6.3.x and earlier
- Avaya Aura® Utility Services (US) 7.0.x and earlier
- Avaya Aura® Media Server (AAMS) 7.7 and earlier
- Avaya Aura® Communication Manager Messaging (CMM) 6.3.x and earlier
- Avaya Aura® Messaging (AAM) 6.3.x and earlier
- Communication Server 1000 Release 7.6 Service Pack 10 and earlier
- IP Office 9.0.x and earlier

Problem description

The Internet Engineering Task Force (IETF) TLS working group has authored and adopted an Internet-Draft to deprecate TLS 1.0 and TLS 1.1. From the abstract:
"These versions lack support for current and recommended cipher suites, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. TLSv1.2 has been the recommended version for IETF protocols since 2008, providing sufficient time to transition away from older versions. Products having to support older versions increase the attack surface unnecessarily and increase opportunities for misconfigurations. Supporting these older versions also requires additional effort for library and product maintenance."

Major Browsers have announced that they will stop supporting TLS 1.0 and TLS 1.1 by March 2020. Links for major browsers:

CHROME: https://security.googleblog.com/2018/10/modernizing-transport-security.html
APPLE: https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/
MICROSOFT: https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/
MOZILLA: https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/

Many older End of Manufacturer Support (EOMS) Avaya products are built on platforms that only supported TLS 1.0.
For example, Communication Manager 6.3.x is built on RedHat Enterprise Linux 5.
RHEL 5.x utilizes OpenSSL library version 0.98 which can only support TLS Version 1.0.
Communication Manager 7.x and above are built on updated versions of RHEL. Communication Manager 7.x is built on RHEL 6.
RHEL 6.x supports OpenSSL version 1.0.2 which can support TLS 1.0, 1.1, 1.2.

Avaya applications are dependent on the capabilities of the underlying operating system they run on, e.g., RHEL in the Communication Manager case.
Versions of RHEL that only support TLS 1.0 will not be updated by RedHat.

The following table lists when support for TLS 1.2 was introduced. Note that some products do not have a Web User Interface and will not be impacted by the browser change but utilize TLS for other communications. Others are End of Manufacturer Support and never supported TLS 1.2. Those are flagged as "N/A".

Avaya Aura® Platform Product/Application	**Earliest Release supporting TLS 1.2 for UI**
Avaya Aura® Communication Manager (CM)	7.0
Avaya Aura® System Manager (SMGR) & WebLM	6.3.13 / 7.0

Avaya Aura® Application Enablement Services (AES)	7.0.1
Avaya Aura® Utility Services (US)	7.1
Avaya Aura® Communication Manager Messaging (UCA)	7.0
Avaya Aura® Media Server (AAMS)	7.8
Avaya Aura® Messaging (AAM)	7.0
Communication Server 1000 (CS1K)	7.6 SP 11
IP Office	9.1

Resolution

Customer should upgrade the application to the currently supported release in order to keep the application's security posture updated.

Workaround or alternative remediation

In the interim while upgrading to the currently supported release (the recommended path), the customer would need to allow and utilize older versions of browsers to interact with affected products. Customers must assess, understand and accept the inherent security risks associated with the workaround of utilizing older browser versions.

Remarks

Issue 1 – original publication December 16, 2019.
Issue 2 – Dec 23, 2019 - updated to include AAM.
Issue 3 – Dec 24, 2019 – updated to include CS1000.
Issue 4 – Feb 12, 2020 – updated to include IP Office.

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

n/a

Patch install instructions

n/a

Service-interrupting?

No

Verification

n/a

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

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.