Product Support Notice

PSN #	PSN020550u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 14-Dec-21. This is issue #08, published date 03-Feb-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN020550u - Avaya Aura® Session Manager Log4j vulnerabilities

Products affected

Avaya Aura® Session Manager, Releases 8.x, 10.1

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security* - ***Apache Log4j Vulnerability - Impact for Avaya products*** on support.avaya.com for updates.

- Session Manager/Branch Session Manager versions earlier than 8.0.0 are not impacted by the Log4j 2.x vulnerabilities.
- Session Manager/Branch Session Manager versions 8.x releases will be flagged on security scans as vulnerable. Avaya is providing a patch to address all 8.x releases to address these vulnerabilities. Reference the Resolution section of this PSN.
- Session Manager/Branch Session Manager 10.1 will be flagged on security scans as vulnerable, and Avaya has provided an updated, mandatory Service Pack to address these vulnerabilities. Reference the Resolution section of this PSN.
- Internal analysis has determined that Session Manager 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in the software. This is because JMSAppender is not used in any of the log4j configurations for Session Manager.
- Internal analysis has determined that Session Manager 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2021-44832 if the latest patches/Service Pack noted in the Resolution Section of this PSN are applied.
- Internal analysis has determined that Session Manager 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is used in the software. This is because JMSSink is not used or configured in any of the log4j configurations for Session Manager by default
- Internal analysis has determined that Session Manager 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23305 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used or configured in any of the log4j configurations for Session Manager by default.
- Internal analysis has determined that Session Manager 8.x and 10.1 releases are not vulnerable to the associated vulnerability CVE-2022-23307 (Log4j 1.x Chainsaw) although Log4j 1.x is used in the software. This is because Chainsaw is not used or configured in any of the log4j configurations for Session Manager by default.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.

Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

Session Manager/Branch Session Manager 8.x; 10.1

Updated Feb 3, 2022: Addition of CVE-2022-23302, CVE-2022-23305 and CVE-2022-23307.

Updated Jan 5, 2022: Addition of CVE-2021-44832 and CVE-2021-4104.

Updated Dec 23, 2021: An updated, mandatory Session Manager Service Pack 0.1 that replaces the original required Session Manager Service Pack 0 has been created. This updated service pack, Session_Manager_10.1.0.0.1010019.bin, includes

everything in Service Pack 0 and mitigation of the Log4j vulnerabilities. Service Pack 0.1 can be applied on top of the previous Service Pack 0.

Updated Dec 22, 2021: A ***new patch*** Session_Manager_87720-300.bin has been created for 8.1.3.3 only.
Session Manager 8.1.3.3 has a different version of the third-party vendor software that contains Log4j compared to the version in 8.1.3.2 and earlier.
While patch Session_Manager_87720-200.bin removed all log4j-2.x jar files in 8.1.3.3, there were still artifacts of these jar files located in the patch backup directory. This presents no exposure to the vulnerabilities, but the presence of these jar files could be flagged on a security scan.
The new patch for 8.1.3.3, Session_Manager_87720-300.bin, contains everything in Session_Manager_87720-200.bin, plus provides for removal of the log4j-2.x jar files from the backup directory.
This is not an issue with Session Manager 8.1.x releases < 8.1.3.3 since they utilize an earlier version of the third-party vendor software and these jar files are not present in the backup directory after application of Session_Manager_87720-200.bin.
Customers who are on Session Manager 8.0.x and 8.1.x <8.1.3.3 do not need to update to this new patch if they have already installed Session_Manager_87720-200.bin.

Updated Dec 18, 2021: *Third party vendor software that contains Log4j and is utilized by Session Manager has provided an additional update, therefore a* ***new patch*** *has been created.*
Session_Manager_87720-003.bin (PLDS ID SM000000217) has been deprecated. Please utilize the new patch with new PLDS ID listed below.

Note: The patch Session_Manager_87720-200.bin is applicable for both Release 8.0.x and 8.1.x.

These patches address all of the Log4j vulnerabilities cited in the Problem Description section of this PSN.

Session Manager/ Branch Session Manager Release	**PLDS Download Information**
8.0.x	**PLDS Download ID:** SM000000218 **File Name:** Session_Manager_87720-200.bin **md5sum:** 85de552447fd3329fcb8a3d8629f9e7a
8.1.x <8.1.3.3	**PLDS Download ID:** SM000000218 **File Name:** Session_Manager_87720-200.bin **md5sum:** 85de552447fd3329fcb8a3d8629f9e7a
8.1.3.3	**PLDS Download ID:** SM000000219 **File Name:** Session_Manager_87720-300.bin **md5sum:** 6ee9eb40bb555959b33cfd2e01e633b6
10.1	***Service Pack 0.1*** **PLDS Download ID:** SM000000220 **File Name:** Session_Manager_10.1.0.0.1010019.bin **md5sum:** cfae81cf020c6f6e6866faf70603478e

Reference the Patch Notes section of this PSN for installation instructions.

Workaround or alternative remediation

N/A

Remarks

PSN Revision History:
Issue 1 – December 14, 2021: Initial publication.
Issue 2 – December 17, 2021: Patch is available for 8.x.
Issue 3 – December 18, 2021: Updated Patch, new PLDS ID due to additional update provided by third party vendor software that contains Log4j and is utilized by Session Manager. Apache link added to Security Risk section.
Issue 4 – December 22, 2021: New patch for 8.1.3.3 only to ensure removal of Log4j jar file artifacts.

Issue 5—December 23, 2021: Patch is available for 10.1.
Issue 6 – January 05, 2022: CVE-2021-4104 and CVE-2021-44832 added.
Issue 7 – January 22, 2022: Updated with additional verification information.
Issue 8 – Feb 03, 2022: CVE-2022-23302, CVE-2022-23305, CVE-2022-23307 added.

Patch Notes

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

Backup before applying the patch

Always

Download

Note: The same patch is applicable for Release 8.0.x and 8.1.x.

Session Manager/ Branch Session Manager Release	PLDS Download Information
8.0.x	**PLDS Download ID:** SM000000218 **File Name:** Session_Manager_87720-200.bin **md5sum:** 85de552447fd3329fcb8a3d8629f9e7a
8.1.x <8.1.3.3	**PLDS Download ID:** SM000000218 **File Name:** Session_Manager_87720-200.bin **md5sum:** 85de552447fd3329fcb8a3d8629f9e7a
8.1.3.3	**PLDS Download ID:** SM000000219 **File Name:** Session_Manager_87720-300.bin **md5sum:** 6ee9eb40bb555959b33cfd2e01e633b6
10.1	***Service Pack 0.1*** **PLDS Download ID:** SM000000220 **File Name:** Session_Manager_10.1.0.0.1010019.bin **md5sum:** cfae81cf020c6f6e6866faf70603478e

Patch install instructions

Service-interrupting?

Yes

For Session Manager 10.1, reference ***Avaya Aura® Release Notes*** for instructions on the Service Pack installation. Service Pack 0.1 can be applied on top of Service Pack 0.

For Session Manager 8.x, patches can be applied on top of one another. For example, if the Session Manager is on 8.1.3.3, and an earlier patch, say Session_Manager_87720-003.bin, had already been installed, Session_Manager_87720-300.bin can be applied on top of it.

- Patch installation using SDM is not supported.
- Take a snapshot of the VM before applying the patch.
- Using the customer admin account, copy the patch to the customer admin home directory.
- Apply the patch using **patchSM <path to patch>** For example:

```
patchSM -i Session_Manager_87720-200.bin
```

- Output should be similar to the following. This example the command is executed within the customer admin home directory where the patch was previously copied.

```
$ patchSM -i Session_Manager_87720-200.bin

Verifying signature...
[  OK  ]

Extracting files
```

```
WARNING Installing patch 87720 will cause a service
interruption. It
is strongly recommended that patches be applied when the
system is idle.

Do you wish to continue (y/N)? y
Stopping Session Manager before installing patch.
Installation started
Starting installation of patch 87720
Installation completed
```

- Remove the snapshot or rollback

Verification

Verify the swversion output.

This is an example for 8.1.3.2 with Session_Manager_87720-200.bin

```
Avaya Aura Session Manager Software Version Inventory

          Application Name: Session Manager
                   Release: 8.1.0.0.810007
Patches:

ID                    Version         Status    Summary
--------------------- --------------- --------- --------------------------------
8.1.3.2               8.1.3.2.813207 installed 8.1.3.2 Service Pack
8.1-SSP-08001         08001          installed Security Service Pack #8
87720                 200            installed Log4j Patch (release 2)
```

This is an example for 8.1.3.3 with Session_Manager_87720-300.bin

```
Avaya Aura Session Manager Software Version Inventory

          Application Name: Session Manager
                   Release: 8.1.0.0.810007
Patches:

ID                    Version         Status    Summary
--------------------- --------------- --------- --------------------------------
8.1-SSP-08001         08001          installed Security Service Pack #8
8.1.3.3               8.1.3.3.813310 installed 8.1.3.3 Service Pack
87720                 300            installed Log4j Patch (release 3)
```

For all Session Manager releases listed in the Resolution Section of this PSN, after application of the update, to confirm that any artifacts related to Log4j are removed, ensure that the following files are no longer present.

```
/opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar
/opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-api-2.8.2.jar
/opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-1.2-api-2.8.2.jar
/opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-slf4j-impl-2.8.2.jar
```

For Session Manager Version 8.1.3.3 and 10.1 , in addition to removal of files mentioned above, the following file will be added

after patch application:

```
/opt/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/slf4j-jdk14-1.7.7.jar
```

Failure

Contact Avaya Services.

Patch uninstall instructions

This patch can only be removed by reverting to a snapshot taken prior to applying the patch.

Security Notes

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

Security risks

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23302
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23307

Reference https://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

As noted in this PSN.

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.