Product Support Notice

PSN #	PSN005937u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is issue #05, published date: 03-Jan-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005937u – Avaya Interaction Center Log4j2 vulnerabilities

Products affected

Avaya Interaction Center, all releases

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) 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

Avaya Interaction Center Releases 7.3.* are running Log4jv1 that are not susceptible.
Internal analysis has determined that this release is not vulnerable to the related Log4j1x plus JMSAppender vulnerability.
It is possible to exploit using JMSAppender as configuration settings could make JNDI function the same as it does in log4j 2.x. (CVE-2021-4104).
In IC OOTB this JMSAppender is not configured. We recommend checking all log4j.xml files on your IC systems to make sure that this appender has not been added manually.

Avaya Interaction Center Release 7.3.9 is impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45105. IC Release 7.3.9 uses log4j v2.13.0 for CSPortal component. As this release uses JDK 8u181, it is vulnerable and may be potentially attacked.

Avaya Interaction Center Release 7.3.10 is impacted by the Log4j2 vulnerabilities CVE-2021-44228, CVE-2021-45105. IC Release 7.3.10 uses log4j v2.13.0 for CSPortal component, but this release also uses JDK 8u292, so it should mitigate CVE-2021-44228, but not CVE-2021-45105.

If you have already upgraded Log4J 2.13 to 2.16.0 or 2.17.0, you must upgrade it once again to 2.17.1 version (see Resolution section) due to CVE-2021-44832 for 2.17.0 version.

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

The patch for CS Portal release versions 7.3.9 and 7.3.10 is available on Avaya Support - Downloads - HF_IC739_IC7310_log4j2_CVE-2021-44228 - Interaction Center. This patch is for CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832.

Workaround or alternative remediation

- For log4j 1.x, does not have Lookups so the risk is lower. Applications using Log4j 1.x are only vulnerable to this attack when they use JNDI in their configuration. Configurations without JMSAppender, not configured in logging configuration, are not impacted by this vulnerability.

- For log4j versions 2.10 and later (IC Releases 7.3.9 and 7.3.10):

CVE	Mitigation
CVE-2021-44228	Remove the JndiLookup class from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.
CVE-2021-45046	Remove the JndiLookup class from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.
CVE-2021-45105	Remove **JndiLookup.class** from the classpath: • zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class. **The following mitigation does not fix the issue completely:** • **Replace Context Lookups with Thread Context Map Patterns** • **Remove References to Context Lookups in Pattern Layout in Logging Configuration file**

Additional Notes:

- CVE-2021-45046 can be mitigated through:
  - For log4j 2.x, remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class.
  - For log4j 1.x, does not have Lookups so the risk is lower. Applications using Log4j 1.x are only vulnerable to this attack when they use JNDI in their configuration. Configurations without JMSAppender, not configured in logging configuration, are not impacted by this vulnerability.
- JMSAppender should not be configured.
- Disable Java system properties for remote class loading via JNDI object factories stored in naming and directory services. This should be default for Java versions of 8u121 and later but should be checked in code:
  1. Set com.sun.jndi.rmi.object.trustURLCodebase to false
  2. Set com.sun.jndi.cosnaming.object.rustURLCodebase set to false.

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 15, 2021: Added patch info.
Issue 3 – December 17, 2021: Added info related to CVE-2021-45046.
Issue 4 – December 21, 2021: Added info related to CVE-2021-45105, updated *Workaround* section.
Issue 5 – January 3, 2022: Added info related to CVE-2021-44832 and CVE-2021-4104.

Patch Notes

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

Backup before applying the patch

Always

Download

The patch for CS Portal release versions 7.3.9 and 7.3.10 is available:
Avaya Support - Downloads - HF_IC739_IC7310_log4j2_CVE-2021-44228 - Interaction Center

Patch install instructions	Service-interrupting?
1) Stop CSPortal service. 2) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-api-2.x.x.jar and replace this file with the log4j-api-2.17.1.jar file from this patch. 3) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-core-2.x.x.jar and replace this file with the log4j-core-2.17.1.jar file from this patch. 4) Backup file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-slf4j-impl-2.x.x.jar and replace this file with the log4j-slf4j-impl-2.17.1.jar file from this patch. 5) Start CSPortal server.	Yes

Verification
Make sure CSPortal writes logs as earlier

Failure
n/a

Patch uninstall instructions
1) Stop CSPortal server. 2) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-api-2.x.x.jar 3) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-core-2.x.x.jar 4) Restore the backed up file <Avaya_IC73_home>\comp\csportal\WEB-INF\lib\log4j-slf4j-impl-2.x.x.jar 5) Start CSPortal server.

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

Avaya Security Vulnerability Classification
Reference www.avaya.com/emergencyupdate

Mitigation
As noted in this PSN.