Product Support Notice

PSN #	PSN005981u

Original publication date: 24-Dec-21. This is issue #03, published date: 07-Jan-22.

Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005981u – Avaya Aura® Workforce Optimization Log4j vulnerabilities

Products affected

Avaya Aura® Workforce Optimization (AAWFO), 15.1.

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) 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 Aura® Workforce Optimization 15.1 is impacted by the Log4j2 vulnerability. Note that AAWFO 15.1 is End of Manufacturer Support for Software since 31-Oct-21. The relevant End of Sale Notice is on Avaya Support Portal since 17-Dec-19.

Software patch updates are needed in certain components of the AAWFO 15.1 solution to upgrade the Apache Log4j2 library from 2.x to 2.16.0 to address vulnerabilities in CVE-2021-44228 and CVE-2021-45046 as defined in the National Vulnerability Database.

CVE-2021-45105 refers to vulnerability in Apache Log4j2 allowing uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. Verint do not use Context Lookups in the AAWFO 15.1 HFR5 and above solution, hence CVE-2021-45105 vulnerability is not applicable to AAWFO 15.1 HFR5 and above.

AAWFO 15.1 HFR5 and above are not vulnerable to the associated vulnerability CVE-2021-44832 (RCE attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server). This is because JDBC Appender is not used in any of the log4j configurations for AAWFO 15.1 HFR5 and above.

AAWFO 15.1 HFR5 and above are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in the Avaya Contact Recorder (ACR) software. This is because JMSAppender is not used in any of the log4j configurations for AAWFO 15.1 HFR5 and above.

The software updates listed below apply to AAWFO 15.1 HFR5, i.e. AAWFO 15.1 Feature Pack 2 (15.1.2).

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 following table lists the specific software patches (KBs) and kits needed to address the Apache Log4j2 vulnerabilities in AAWFO 15.1 HFR5. These software updates can be accessed through the Avaya Support portal / PLDS or through the Verint Software Download page in Verint Connect.

Product Category	Subsystem	PLDS ID	Patch or Kit Number
WFO Suite	Oracle WebLogic	WFO000001058	Security Kit 20b (KB126538)
Enterprise Recording	ArchiveWS_IIS	WFO000001059	KB126539
Analytics	Text Analytics Application	WFO000001060	KB126536
Mobile	Mobile Gateway	WFO000001057	KB202394

Workaround or alternative remediation
N/A

Remarks
PSN Revision History Issue 1 – December 24, 2021: Initial publication. Issue 2 – January 06, 2022: Updated for two further CVEs – both are N/A for AAWFO. Issue 3 – January 07, 2022: Title updated.

Additional Deployment Notes

KB Uninstall Directory Contains Vulnerable Files.

For patch\directory information given below, for Avaya Aura® Workforce Optimization installations, the *%IMPACT360SOFTWAREDIR%* directory is *AvayaAura\Software.*

Verint uses the directories in the %IMPACT360SOFTWAREDIR%\hotfixes directory to store previously installed versions of the product. The files in these directories are only used to roll back an installed KB to a previous version.
When a new component (KB) is installed on a Verint server, the existing files (pre-KB install) are backed up to the hotfixes folder.
If the KB is ever rolled back to the previous version, then the backed-up versions from the hotfixes folder will be placed back into the production folders.
When the Hotfix Deployment Fix Tool (HDFT) runs, a process removes entries from the hotfixes folder if the rollback entry is more than 6 months old and the e: drive disk free space is below predetermined thresholds.
If a KB is installed to address a vulnerability in the product, old versions of vulnerable executables are placed in the hotfixes folder. Old versions are kept for the roll back process to work and are not used by the WFE software. If customers wish to remove all copies of the vulnerable files on the server, they can remove any of the KB###### folders. However, removing these folders also removes the ability to uninstall the KBs associated with those rollback folders.

Oracle Weblogic Patch Uninstall Directory Contains Vulnerable Files

Product updates to the Oracle WebLogic component place old Oracle WebLogic patches in the %IMPACT360SOFTWAREDIR%\ProductionServer\.patch_storage directory. Similar to Verint's hotfixes directory, these are used to rollback WebLogic patches if necessary and are not used by the WFE software. Removal of specific patch directories removes the ability to rollback Oracle WebLogic patches.

Oracle WebLogic Update

The following filename that exists on the system may cause confusion:

%IMPACT360SOFTWAREDIR%\ProductionServer\oracle_common\modules\thirdparty\log4j-2.11.1.jar	Oracle Weblogic have addressed the vulnerability by upgrading log4j in place. Inspection of the manifest file contents will show that the contents are actually the log4j-core-2.16.0.jar
%IMPACT360SOFTWAREDIR%\ProductionServer\oracle_common\modules\thirdparty\features\log4j.jar	This file does not contain any executable classes and is therefore not vulnerable.

Patch Notes

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

Backup before applying the patch
Always

Download
n/a.

Patch install instructions	Service-interrupting?
n/a	Yes

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

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.

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.