Product Support Notice

PSN # PSN005942u

Original publication date: 31-Jan-2022. This is issue #05, published date: 31-Jan-2022.

Severity/risk level: High | Urgency: Immediately

Name of problem

Avaya Workforce Engagement Select Log4j2 vulnerability (CVE-2021-44228) (CVE-2021-45046) (CVE-2021-45105) (CVE-2021-44832) (CVE-2021-4104) (CVE-2022-23302), (CVE-2022-23305), (CVE-2022-23307)

Products affected

Avaya Workforce Engagement Select, 5.3

Avaya Workforce Engagement Select, 5.3.0.1

Avaya Workforce Engagement Select, 5.3.0.2

Note: Avaya Workforce Engagement Select (AWES) was previously known as Avaya Workforce Engagement Select (AWFOS).

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

- AWES versions earlier than 5.3.0 are not impacted by the Log4j2 vulnerability (CVE-2021-44228) as all the components are using Log4j1x which is not vulnerable.
- The only components that are impacted from 5.3 and above are AvayaAdapter (DevLinkAdapter, OceanaAdapter, MLSAdapter, IPOCCAdapter, POMAdapter) and CiscoAdapter and we are giving a Log4j 2.16 jar files as patch for remediation.

AWES	5.3.0.2	5.3.0.1	5.3.0	5.2 - 5.2.x	5.1 – 5.1.x	5.0 – 5.0.x	Comments
CVE-2021-44228	**Yes**	**Yes**	**Yes**	**No**	**No**	**No**	**Yes- log4j2.13 is used** **No- Log4j1.x is used**
CVE-2021-45046	**Yes**	**Yes**	**Yes**	**No**	**No**	**No**	**Yes- log4j2.13 is used** **No- Log4j1.x is used**
CVE-2021-45105	**No**	**No**	**No**	**No**	**No**	**No**	**No- Context lookups are not configured and used**
CVE-2021-44832	**No**	**No**	**No**	**No**	**No**	**No**	**No- We are not using JDBC Appender in our configuration of log4j2 versions > 2. So not impacted**

Important Notes:

- Internal analysis has determined that AWES releases are not vulnerable to the related Log4j 1.x JMSAppender and JNDILookups vulnerability as they are not used and configured for the product in the system.
- Internal analysis has determined that AWES releases which are upgraded to Log4J 2.16 with this patch are not vulnerable for CVE-2021-45105 because the context user is not configured and not used in the product.
- It is recommended that Java run time at customers should be running at Java 6 – 6u212, Java 7 – 7u202,Java 8 – 8u192,Java 11 - 11.0.2 and above

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

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

Internal analysis has determined that AWES 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 AWES by default.

Internal analysis has determined that AWES 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 AWES by default.

Internal analysis has determined that AWES 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 AWES by default.

Internal analysis has determined that AWES 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 AWES 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

AWES versions earlier than 5.3.0 is not impacted by this vulnerability, hence no action needed.
AWES versions 5.3.0 and above, please download the patch from this link and apply as per steps mentioned below:
AWES all versions uses Log4j 1.x but not configured with JMS Sink, JMSAppender and Chainnsaw, so no impact

Workaround or alternative remediation

Remarks

PSN Revision History
Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 17, 2021: Updated publication with link to patch in Resolution section and used version PSN template.
Issue 3 – December 21, 2021: Updated publication with rollback steps and used version 4 PSN template.
Issue 4 – January 07, 2022: Updated publication with rollback steps and used version 5 PSN template
Issue 5 – January 31, 2022: Updated publication with rollback steps and used version 6 PSN template

Patch Notes

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

Backup before applying the patch

Always

Download

Patch download link for Avaya Workforce Engagement Select, 5.3 and above

AWES-Log4J patch-Download

Patch install instructions — Service-interrupting?

Steps to apply the fix\patch: Yes

1. Stop the AvayaAdapter\ DevLinkAdapter\ OceanaAdapter\ MLSAdapter\ IPOCCAdapter\ POMAdapter\ CiscoAdapter from services.msc.
2. Unzip the patch provided.
3. Navigate to the <Installation_folder>\AWFOS5\<Adapter>\lib and
    a. Remove the log4j-api-2.13.0.jar, log4j-core-2.13.0.jar and log4j-slf4j-impl-2.13.0.jar and take backup.
    b. Copy the files from unzipped patch folder to the above location
4. Start the Adapter in the services.msc
5. Check if it is starting properly and writing the log files

Verification

Please see if the components are up and running and writing log files properly

Failure

If you see any failure cases in applying the patch. Just revert the patch and contact Avaya Workforce Engagement Select Support Team.

Patch uninstall instructions

1. Stop the service in services.msc, for which you applied the jar files\patch.
2. Remove the applied jar files and copy the old ones which you took backup before applying this patch.
3. Start the service in the services.msc.
4. Verify that this component is writing the logs properly.

And contact Avaya Workforce Engagement Select Support Team for help in 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
Reference https://logging.apache.org/log4j/1.2/

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.