Product Support Notice

PSN #	PSN005959u	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: 07-Jan-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005959u – Avaya Business Rules Engine – Log4j2 vulnerabilities.

Products affected

Avaya Business Rules Engine (BRE) 3.3, 3.4, 3.5, 3.6, 3.7

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

BRE is not directly impacted by the Log4j 2.x vulnerabilities but there are affected class files in third-party open-source libraries that are included with the BRE software.

BRE is running Log4j 1.x that is not susceptible.

Internal analysis has determined that this release is not vulnerable to the CVE-2021-4104 (Log4j 1.x JMSAppender) vulnerability although Log4j 1.x is used in the software. This is because JMSAppender is not used in any of the log4j configurations for Business Rules Engine.

To prevent future potential security issues and to protect the systems in general, Avaya recommends applying the patch file on all BRE servers.

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

Download and install the patch to each BRE server. Every server in the solution needs to be updated.

If a customer cannot install the patch for some reason, a workaround is provided to manually remove the affected class files.

Scanning software that looks for specific versions of Log4j jar files will still indicate a potential vulnerability. This is because the affected JAR versions remain even if the vulnerable class files have been removed.

Workaround or alternative remediation

Manual actions to mitigate the log4j class file vulnerability:

Perform the following steps on each BRE server:

1. Log into each BRE server as the root user (or log in as a regular user and su to root).
2. Make sure the zip command is installed and available in the path:

```
zip -version
```

If it is not installed, please install it first using:

```
yum install zip
```

Or download and manually install the corresponding RPM.

3. Stop the abre-services:

   ```
   systemctl stop abre-services
   ```

   For BRE 3.3 the commands to stop the services are:

   ```
   stop dr/cluster-services
   stop dr/zookeeper
   stop dr/kafka-instance conf=local
   stop dr/elastic
   stop dr/logstash
   ```

4. Change to the directory above the BRE home directory:

   ```
   cd {ABRE_HOME}/../
   ```

   If BRE is installed in the default location this will be /opt/Avaya/

5. Find all the log4j-core.jar file locations:

   ```
   find . -name log4j-core*.jar
   ```

   The output should be similar to this:

   ```
   ./third-party/logstash/logstash-6.3.2/logstash-core/lib/jars/log4j-core-2.9.1.jar
   ./third-party/elasticsearch/elasticsearch-6.8.8/lib/log4j-core-2.11.1.jar
   ```

6. For each of the locations found, execute the following command to remove the JNDI lookup class:

   ```
   zip -q -d {PATH_TO_LOG4J} org/apache/logging/log4j/core/lookup/JndiLookup.class
   ```

   For example:

   ```
   zip -q -d ./third-party/logstash/logstash-6.3.2/logstash-core/lib/jars/log4j-core-
   2.9.1.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

   zip -q -d ./third-party/elasticsearch/elasticsearch-6.8.8/lib/log4j-core-2.11.1.jar
   org/apache/logging/log4j/core/lookup/JndiLookup.class
   ```

7. Start the abre-services.

   ```
   systemctl start abre-services
   ```

   For BRE 3.3 the commands to start the services are:

   ```
   start dr/cluster-services
   start dr/zookeeper
   ```

```
start dr/kafka-instance conf=local
start dr/elastic
start dr/logstash
```

Remarks

n/a

Patch Notes

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

Backup before applying the patch

It is recommended that the BRE servers be backed up before applying the patch or workarounds.

Download

The Download can be obtained from these locations:

PLDS:
Download pub ID: BRE000000031

https://downloads.dlavaya.com/ABRE/abre-log4j-patch.sh?fileExt=.sh&__dlmt__=1639758502_e658d833ae3043215124603d452d729d

Support.avaya.com:

https://support.avaya.com/products/P1638/business-rules-engine/All

Patch install instructions

Service-interrupting?

Yes

Perform the following steps on each BRE node:

1. Log into each BRE server as the root user (or log in as a regular user and su to root).
2. Make sure the zip command is installed and available in the path:

   ```
   zip -version
   ```

   If it is not installed, please install it first using:

   ```
   yum install zip
   ```

   Or download and manually install the corresponding RPM.
3. Stop the abre-services:

   ```
   systemctl stop abre-services
   ```

   For BRE 3.3 the commands to stop the services are:

   ```
   stop dr/cluster-services
   stop dr/zookeeper
   ```

```
stop dr/kafka-instance conf=local
stop dr/elastic
stop dr/logstash
```

4. Download the patch file, fix the permissions, and run it:

   ```
   chmod +x ./abre-log4j-patch.sh
   ```

   ```
   ./abre-log4j-patch.sh
   ```

   IMPORTANT! Be sure to populate the Avaya path (by default /opt/Avaya).

   This script will find all log4j-core.jar libraries and remove the JndiLookup.class from them.

5. Start the abre-services.

   ```
   systemctl start abre-services
   ```

   For BRE 3.3 the commands to start the services are:

   ```
   start dr/cluster-services
   start dr/zookeeper
   start dr/kafka-instance conf=local
   start dr/elastic
   start dr/logstash
   ```

Verification

To verify that vulnerable JndiLookup.class was removed you can do one of the following:

1. Log into each BRE server as the root user (or log in as a regular user and su to root).
2. Change to the directory above the BRE home directory:

   ```
   cd {ABRE_HOME}/../
   ```

   If BRE is installed in the default location this will be /opt/Avaya/

3. Find all the log4j-core.jar file locations:

   ```
   find /opt/Avaya -name log4j-core*.jar
   ```

   The output should be similar to this:

   ```
   ./third-party/logstash/logstash-6.3.2/logstash-core/lib/jars/log4j-core-2.9.1.jar
   ./third-party/elasticsearch/elasticsearch-6.8.8/lib/log4j-core-2.11.1.jar
   ```

4. Run this command on each jar file location:

   ```
   jar tvf <lib_location of log4j-core-*.jar> | grep -i JndiLookup
   ```

   The output should be empty if the vulnerable class is not found:

```
[root@abre-1 ~]# find /opt/Avaya/ -name "log4j-core*jar"
/opt/Avaya/third-party/logstash/logstash-6.3.2/logstash-core/lib/jars/log4j-core-
2.9.1.jar
/opt/Avaya/third-party/elasticsearch/elasticsearch-6.3.2/lib/log4j-core-2.9.1.jar

[root@abre-1 ~]# jar tvf /opt/Avaya/third-party/logstash/logstash-6.3.2/logstash-
core/lib/jars/log4j-core-2.9.1.jar | grep -i JndiLookup

[root@abre-1 ~]# jar tvf /opt/Avaya/third-party/elasticsearch/elasticsearch-
6.3.2/lib/log4j-core-2.9.1.jar | grep -i JndiLookup
```

Failure

If the script is run a second time or if there are no vulnerable libraries found, the output will display the message "zip error: Nothing to do!"

```
[root@linpubac131 ~]# ./abre-log4j-patch.sh
#==========================================================================
This script is created for BRE 3.3, 3.4, 3.5, 3.6 and 3.7 versions.
It will mitigate vulnerability CVE-2021-44228 for Log4j2 <=2.14.1
Important! You should input the Avaya path folder (/opt/Avaya), it is not the ABRE
(/opt/Avaya/abre) folder!
#==========================================================================

Please enter Avaya installation path [/opt/Avaya]:
Found place with log4j-core:
/opt/Avaya/third-party/logstash/logstash-5.6.1/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.6.2/log4j-core-2.6.2.jar

zip error: Nothing to do! (/opt/Avaya/third-party/logstash/logstash-
5.6.1/logstash-core/lib/org/apache/logging/log4j/log4j-core/2.6.2/log4j-core-
2.6.2.jar)

Found place with log4j-core:
/opt/Avaya/third-party/elasticsearch/elasticsearch-5.2.0/lib/log4j-core-2.7.jar

zip error: Nothing to do! (/opt/Avaya/third-party/elasticsearch/elasticsearch-
5.2.0/lib/log4j-core-2.7.jar)

All found places have been fixed.
```

Patch uninstall instructions

Revert to the backup that was taken earlier.

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.