Product Security Advisory: Apache Log4j - CVE-2021-44228

Sierra Wireless Advisory: SWI-PSA-2021-007 (link to latest version)

Issued: December 14, 2021 1:15 p.m. PST

Last Updated January 14, 2022 5:30 p.m. PST

Summary

The Sierra Wireless security team has completed a comprehensive review to determine the impact on our products and services. of CVE-2021-44228 and the follow-on vulnerability CVE-2021-45046, published December 14th.

> **CVE-2021-44228**: a remote code execution vulnerability in Apache Log4j. It is remotely exploitable without authentication, i.e., may be exploited over a network without the need for a username and password. https://nvd.nist.gov/vuln/detail/CVE-2021-44228
>
> **CVE-2021-45046**: a new vulnerability reported against Log4j that is dependent on specific non-standard configurations.

Our review has determined that the vulnerable log4j code identified by these CVEs was present in our AM/AMM servers as well as certain internal components of our AirVantage® and Octave™ cloud platforms. However, these systems do not operate with the specific non-standard configuration required for CVE-2021-25046 and hence were not vulnerable to it.

Affected Products and Services

Our comprehensive review is complete and the Sierra Wireless Products and Services that were affected by these log4j vulnerabilities are listed below. Our review found no other Sierra Wireless products or services that were affected.

On-premises AM/AMM Product: We are recommending that all customers with on-premises AM/AMM servers that have access from the public internet temporarily disable those servers until a remediation patch can be applied. Sierra Wireless is actively working on documenting a patching process that will allow on-premises customers to quickly patch their systems and return them to normal operation. We are recommending that all on-premises customers, whether their servers have access to the public internet or not, follow the remediation process set out below to apply the recommended security patch. Please contact Technical Support at the details set out below for further information.

Hosted AMM Services: Out of an abundance of caution, Sierra Wireless has suspended access to our Hosted AMM servers to reduce the impact of this issue while we complete the required security patches. Once the servers have been updated, services will be returned to a normal operational state and further communication will be provided. Hosted AMM customers can refer to https://status.sierrawireless.com/ for updates on our remediation efforts.

AirVantage and Octave Cloud Platforms: Our review of these platforms has indicated that Apache Log4j is only used by select internal components of these platforms. Further, we have been unable to identify a mechanism by which an attacker could submit a malicious payload and have it processed by log4j through these platforms. Regardless, we have applied the recommended security patches for the log4j issue and these platforms are in service.

Scope of Impact

Vulnerable servers may be triggered to download and execute malware.

Remediation Actions

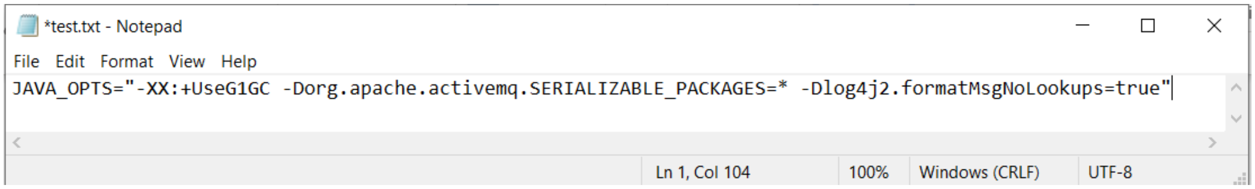
Sierra Wireless has implemented a patch for the AM/AMM on-premises server software that customers can apply to mitigate the log4j vulnerability. This approach has been tested and validated on three versions of the AM/AMM software, and Sierra Wireless recommends that customers follow the instructions below for your version of the AM/AMM software.

Important: When making changes to the system files (e.g. section 1.2 below), the new entry must not include any extra characters/line breaks such as is shown in the examples below. Due to the formatting of this document, we recommend that the input is sanitized using a text editor rather than copying and pasting from this document.

As an example, in section 1.2 for the instructions below, the entry from this document

```
JAVA_OPTS="-XX:+UseG1GC ·-
Dorg.apache.activemq.SERIALIZABLE_PACKAGES=* ·-
Dlog4j2.formatMsgNoLookups=true"¶
```

Should be formatted as



```
JAVA_OPTS="-XX:+UseG1GC -Dorg.apache.activemq.SERIALIZABLE_PACKAGES=* -Dlog4j2.formatMsgNoLookups=true"
```

AM/AMM 2.17.1.x

There are three services that require updates on AM/AMM 2.17.1x. To complete the update please make all three changes:

Open an SSH session to the server and make the following changes as the root user:

1. Tomcat

1.1. Backup Tomcat

```
cd /etc/tomcat
cp tomcat.conf tomcat.config.orig
vi tomcat.conf
```

1.2. Change the following line:

```
JAVA_OPTS="-XX:+UseG1GC -
Dorg.apache.activemq.SERIALIZABLE_PACKAGES=*"
```

to

```
JAVA_OPTS="-XX:+UseG1GC -
Dorg.apache.activemq.SERIALIZABLE_PACKAGES=* -
Dlog4j2.formatMsgNoLookups=true"
```

Note: Please be cautious when making the edits to ensure you copy the full content above. Line breaks in this document are due to the formatting of the document.

1.3. Save the file and quit.

2. DB loader

2.1 Backup DB loader

```
cd /opt/tomcat/webapps/inmotion/WEB-INF
cp startloader.sh startloader.sh.orig
vi startloader.sh
```

2.2 Add the following line below the entry for "-XX"

```
-Dlog4j2.formatMsgNoLookups=true \
```

Your final entry should look as follows:

```
-classpath
/usr/share/java/dels.jar:/opt/tomcat/webapps/inmotion/WEB-
INF/classes:/opt/tomcat/webapps/inmotion/WEB-INF/lib/* \
-XX:+UseG1GC -Xmx5G \
-Dlog4j2.formatMsgNoLookups=true \
-Dorg.apache.activemq.SERIALIZABLE_PACKAGES=* \
-DPROCESSNAME=imtdbloader \
-Duser.timezone=Canada/Pacific \
-DTIME=120 \
```

2.3 Save the changes and quit.

3. API

3.1 Backup the APIs

```
cd /opt/tomcat/webapps/inmotion/WEB-INF/api/
cp ammapi.sh ammapi.sh.orig
vi ammapi.sh
```

3.2 Add the following line below the entry for "-Xmx"

```
-Dlog4j2.formatMsgNoLookups=true \
```

Your final entry should look as follows:

```
/usr/bin/java \
-XX:+UseG1GC \
-Xmx512M \
-Dlog4j2.formatMsgNoLookups=true \
-Dorg.apache.activemq.SERIALIZABLE_PACKAGES=* \
```

3.3 Save the changes and quit.

4. Restart the AM/AMM

```
ammctl stop
ammctl start
```

Note: You can make the modifications to the AM/AMM while it is running, and then stop and start the services. This will reduce the overall system downtime.

AM/AMM 2.17

There are two services that require updates on AM/AMM 2.17. To complete the update please make both changes:

Open an SSH session to the server and make the following changes as the root user:

1. Tomcat

   1.1. Backup Tomcat

   ```
   cd /etc/tomcat
   cp tomcat.conf tomcat.config.orig
   vi tomcat.conf
   ```

   1.2. Change the following line:

   ```
   JAVA_OPTS="-XX:+UseG1GC"
   ```

   to

   ```
   JAVA_OPTS="-XX:+UseG1GC -Dlog4j2.formatMsgNoLookups=true"
   ```

   1.3. Save the file and quit.

2. DB loader

   2.1 Backup DB loader

```
cd /opt/tomcat/webapps/inmotion/WEB-INF
cp startloader.sh startloader.sh.orig
vi startloader.sh
```

   2.2 Add the following line below the entry for "-XX"

```
-Dlog4j2.formatMsgNoLookups=true \
```

   Your final entry should look as follows:

```
-classpath
/usr/share/java/dels.jar:/opt/tomcat/webapps/inmotion/WEB-
INF/classes:/opt/tomcat/webapps/inmotion/WEB-INF/lib/* \

-XX:+UseG1GC -Xmx5G \

-Dlog4j2.formatMsgNoLookups=true \
```

   2.3 Save the changes and quit.

3. Restart the AM/AMM

```
ammctl stop
ammctl start
```

Note: You can make the modifications to the AM/AMM while it is running, and then stop and start the services. This will reduce the overall system downtime.

AM/AMM 2.16.x

To complete the update please make the following changes to the AM/AMM:

Open an SSH session to the server and make the following changes as the root user:

1. Backup the original jar file:

```
cd /opt/tomcat/webapps/inmotion/WEB-INF/lib

cp log4j-core-2.6.2.jar log4j-core-2.6.2.jar.orig
ls -l log4j*
```

2. Create a new jar file and make sure the new one is of a different size than the old one:

```
zip -q -d log4j-core-*.jar
org/apache/logging/log4j/core/lookup/JndiLookup.class

ls -l log4j*
```

3. Restart the AM/AMM:

```
service monit stop
service tomcat stop
service imtdbloader stop
service imtdbloader start
service tomcat start
service monit start
```

Sierra Wireless will be releasing AM/AMM 2.17.1.5, a formal update to the AM/AMM software that will include these changes.

Support Contact Information

Sierra Wireless Technical Support is available by phone 24/7/365 or via support case submitted to the web portal.
Phone (Toll-Free): 1-877-687-7795
Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:
https://www.sierrawireless.com/company/security/