Log4j2 Vulnerability

Information for customers affected by the CVE-2021-44228.

Dear customers,

Ataccama can confirm that several platform versions contain the recently discovered Log4j2 vulnerability (CVE-2021-44228). Below you may find the details as to which Ataccama modules and versions are affected and how to apply the patch to your specific configuration.

Detailed Description of the Vulnerability and Exploits

https://www.lunasec.io/docs/blog/log4j-zero-day/

Log4j Mitigation Guide

https://lists.apache.org/thread/gzj2jsglvsffzs8zormxyly0vofdxp6j

Version 13.x

This family of versions is vulnerable to CVE-2021-44228 due to its 3rd party dependencies.

The Ataccama components are not vulnerable to CVE-2021-44228. Gen2 doesn't use Log4J as the underlying logging library. SLF4J library is used as the logging abstraction layer and Logback is used in the underlying logging library. The file *log4j-core<version>.jar* containing the vulnerable JndiLookup class is not present on the classpath.

Component	Vulnerable
MMM Backend	No
MMM Frontend	No
DPM	No
DPE	No
Runtime	No
AI Core	No

Configuration service	No
Audit module	No
MDM Web Application	No
MDM Server	No
RDM Web Application	No
DQ Issue Tracker Web Application	No
ONE Desktop	No

Ataccama 3rd party dependencies

These components are used as standalone dependencies.

Component	Vulnerable	Description	Log4j version
Keycloak	No	Keycloak is used as an identity provider for authentication and authorization flows.	
Minio	No	Minio is used as object storage.	
Elasticsearch	VULNERABLE	This is an optional dependency used for search in Gen2 Catalog. This dependency needs to be patched because it is vulnerable.	log4j-core-2.11.1.jar
Manta	VULNERABLE	This is an optional dependency used for data lineage. This dependency needs to be patched because it is vulnerable.	log4j-core-2.13.1.jar

How to patch Elasticsearch

1. Please follow Elasticsearch instructions for setting JVM properties and add the JVM property *log4j.formatMsgNoLookups=true.*
2. Restart Elasticsearch

In addition to this fix we highly recommend deleting the vulnerable class.

1. Locate the vulnerable library log4j-core-*.jar . You can use the following command in the installation directory. *find . -type f -name "log4j-core*.jar"*
    a. The command prints a path to the log4j-core file if it exists. For example: *elasticsearch/lib/log4j-core-2.11.1.jar*
2. Delete the vulnerable class on path. You can use the following command *zip -d PATH_TO_FILE org/apache/logging/log4j/core/lookup/JndiLookup.class*
    a. *zip -d elasticsearch/lib/log4j-core-2.11.1.jar org/apache/logging/log4j/core/lookup/JndiLookup.class*
2. Restart Elasticsearch

How to patch Manta

Two Manta services, the Manta Dataflow Server and Manta Admin UI, require a patch. To do so, please follow the instructions below.

Manta dataflow

1. Go to the Manta installation directory e.g. */opt/ataccama/manta/**server**/bin*
2. Edit *setenv.sh*
    a. Add the following line *export JAVA_OPTS="-Dlog4j.formatMsgNoLookups=true"*
3. Restart Manta service

Manta admin UI

4. Go to the Manta installation directory e.g. */opt/ataccama/manta/**serviceutility**/bin*
5. Edit *setenv.sh*
    a. Add the following line *export JAVA_OPTS="-Dlog4j.formatMsgNoLookups=true"*
6. Restart Manta service

How to check whether Manta has been patched

1. Run the following command *ps -auxw | grep java | grep log4j*
    a. At the output you should find *-Dlog4j.formatMsgNoLookups=true* when is Manta patched

Example:

```
user@host:ps -auxw | grep java | grep log4j


root     1531077  166  5.7 7004788 944796 pts/3  Sl   09:16   1:23
/usr/bin/java
-Djava.util.logging.config.file=/opt/ataccama/manta/server/conf/logging.propert
ies -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Dlog4j.formatMsgNoLookups=true -Djdk.tls.ephemeralDHKeySize=2048
-Djava.protocol.handler.pkgs=org.apache.catalina.webresources
```

```
-Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -Xms512M -Xmx3072M
-Dignore.endorsed.dirs= -classpath
/opt/ataccama/manta/server/bin/bootstrap.jar:/opt/ataccama/manta/server/bin/tom
cat-juli.jar -Dcatalina.base=/opt/ataccama/manta/server
-Dcatalina.home=/opt/ataccama/manta/server
-Djava.io.tmpdir=/opt/ataccama/manta/server/temp
org.apache.catalina.startup.Bootstrap start
```

Version 12.x

This family of versions is vulnerable to CVE-2021-44228.

Ataccama components

The Ataccama Gen1 components are not vulnerable because they do not use Log4J as the underlying logging library. 1

Component	Vulnerable	Log4j version
DQD	No	
DQIT	No	
MDM	No	
RDM	No	
DQC	No	
MDA	No	
Runtime	No	
MDC	No	
IDE	No	
ONE web app (DQ and DG)	VULNERABLE	log4j-core-2.7.jar

Ataccama 3rd party dependencies

Component	Vulnerable	Description	Log4j version
Keycloak	No	Keycloak is used as an identity provider for authentication and authorization flows.	
RabbitMQ	No	Messaging provider	
Elasticsearch	VULNERABLE	This dependency needs to be patched because it is vulnerable.	log4j-core-2.11.1.jar

How to patch ONE web app

1. Delete file INSTALLATION_DIR/one/webapps/ROOT/WEB-INF/lib/log4j-core-2.7.jar/*org/apache/logging/log4j/core/lookup/JndiLookup.class*
    a. You can use the following command *zip -d* INSTALL_DIR/one/webapps/ROOT/WEB-INF/lib/log4j-core-2.7.jar *org/apache/logging/log4j/core/lookup/JndiLookup.class*
2. Restart ONE web app

How to patch Elasticsearch

3. Please follow Elasticsearch instructions for setting JVM properties and add the JVM property *log4j.formatMsgNoLookups=true.*
4. Restart Elasticsearch

In addition to this fix we highly recommend deleting the vulnerable class.

3. Locate the vulnerable library log4j-core-2.7.jar . You can use the following command in the installation directory. *find . -type f -name "log4j-core*.jar"*
    a. The command prints a path to the log4j-core file if it exists. For example: *elasticsearch/lib/log4j-core-2.11.1.jar*
4. Delete the vulnerable class on path. You can use the following command *zip -d PATH_TO_FILE org/apache/logging/log4j/core/lookup/JndiLookup.class*
    a. *zip -d elasticsearch/lib/log4j-core-2.11.1.jar org/apache/logging/log4j/core/lookup/JndiLookup.class*
3. Restart Elasticsearch

Version 11.x

This family of versions is not vulnerable to CVE-2021-44228.

Version 10.x

This family of versions is not vulnerable to CVE-2021-44228.

Version 9.x

This family of versions is not vulnerable to CVE-2021-44228.