HPE IMC Security Advisory

Notification

Apache Log4J2 Vulnerability

Data: December 14, 2021

CVE ID: CVE-2021-44228

Summary

In Apache Log4j2 version 2.14.1 and earlier, JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. This behavior is disabled by default in Log4j2 2.15.0 and later.

In previous releases later than 2.10, this behavior can be mitigated by setting the system property "log4j2.formatMsgNoLookups" to “true,” or by removing the JndiLookup class from the classpath (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class). Java 8u121 (see https://www.oracle.com/java/technologies/javase/8u121-relnotes.html) protects against remote code execution by defaulting "com.sun.jndi.rmi.object.trustURLCodebase" and "com.sun.jndi.cosnaming.object.trustURLCodebase" to "false."

Affected Products

HPE IMC PLAT <= E0706P06

Corrective Action Required (Windows Server)

Customers must take immediate action to prevent potential attackers from using this

exploit. Follow the steps below to mitigate this exploit:

1. Login the IMC server and stop IMC service in the intelligent deployment monitoring agent.
2. Open the **iMC\client\bin** folder.
3. Open the file named **startup.bat** for editing.
4. Loacte the line that starts with: **set JAVA_OPTS=%JAVA_OPTS%**.
5. Add the below at the end of this line.

   -Dlog4j.formatMsgNoLookups=true

   Example before:

   set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=%JMXRMI_PORT% -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.access.file="%IMC_HOME%\bin\jmx.access" -Dcom.sun.management.jmxremote.login.config=JmxConfig -Djava.security.auth.login.config="%IMC_HOME%\bin\jmx.config" -Djavax.net.ssl.keyStore="%IMC_HOME%\security\newks" -Djavax.net.ssl.keyStorePassword=iMCV500R001 -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -Dfastjson.parser.safeMode=true

   Example after:

   set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=%JMXRMI_PORT% -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.access.file="%IMC_HOME%\bin\jmx.access" -Dcom.sun.management.jmxremote.login.config=JmxConfig -Djava.security.auth.login.config="%IMC_HOME%\bin\jmx.config" -Djavax.net.ssl.keyStore="%IMC_HOME%\security\newks" -Djavax.net.ssl.keyStorePassword=iMCV500R001 -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -Dfastjson.parser.safeMode=true **-Dlog4j.formatMsgNoLookups=true**

6. Save the file and start IMC service in the intelligent deployment monitoring agent.

Corrective Action Required (Linux Server)

Customers must take immediate action to prevent potential attackers from using this exploit. Follow the steps below to mitigate this exploit:

1. Login the IMC server and stop IMC service in the intelligent deployment monitoring agent.
2. Change to the **iMC\client\bin** directory.
3. Open the file named **startup.sh** for editing.
4. Loacte the line that starts with: **"$JAVA_HOME/bin/java" -server**.
5. Add the below just before **-jar "$IMC_HOME/bin/bootstrap.jar" start &**.

   -Dlog4j.formatMsgNoLookups=true

   Example before:

   "$JAVA_HOME/bin/java" -server -Xmx4196m -Xrs -Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true -XX:+PrintGCDetails -XX:+TraceClassUnloading -XX:+TraceClassLoading -XX:CompressedClassSpaceSize=3G -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log -Dimc.home="$IMC_HOME" -Duser.language=en -Duser.country=US -Dfile.encoding=GB18030 -Djava.awt.headless=true -Dcom.sun.management.jmxremote.port=9091 -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.access.file=./jmx.access -Dcom.sun.management.jmxremote.login.config=JmxConfig -Djava.security.auth.login.config="$IMC_HOME/bin/jmx.config" -Djavax.net.ssl.keyStore="$IMC_HOME/security/newks" -Djavax.net.ssl.keyStorePassword=iMCV500R001 -Djava.io.tmpdir="$IMC_ROOT/tmp" -Dorg.apache.el.parser.COERCE_TO_ZERO=false -

Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true -Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -Dfastjson.parser.safeMode=true -jar "$IMC_HOME/bin/bootstrap.jar" start &

Example after:

"$JAVA_HOME/bin/java" -server -Xmx4196m -Xrs -Dcom.sun.xml.bind.v2.bytecode.ClassTailor.noOptimize=true -XX:+PrintGCDetails -XX:+TraceClassUnloading -XX:+TraceClassLoading -XX:CompressedClassSpaceSize=3G -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log -Dimc.home="$IMC_HOME" -Duser.language=en -Duser.country=US -Dfile.encoding=GB18030 -Djava.awt.headless=true -Dcom.sun.management.jmxremote.port=9091 -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.access.file=./jmx.access -Dcom.sun.management.jmxremote.login.config=JmxConfig -Djava.security.auth.login.config="$IMC_HOME/bin/jmx.config" -Djavax.net.ssl.keyStore="$IMC_HOME/security/newks" -Djavax.net.ssl.keyStorePassword=iMCV500R001 -Djava.io.tmpdir="$IMC_ROOT/tmp" -Dorg.apache.el.parser.COERCE_TO_ZERO=false -Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true -Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=true -Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true -Dfastjson.parser.safeMode=true **-Dlog4j.formatMsgNoLookups=true** -jar "$IMC_HOME/bin/bootstrap.jar" start &

6. Save the file and start IMC service in the intelligent deployment monitoring agent.

Future Considerations

HPE will release new versions of IMC with appropriate patches for log4j2 library. You must upgrade to the patched version as soon as possible to prevent future variations of this vulnerability.