Silver Peak Security Advisory

Notification

Apache Log4j2 Vulnerability

Date: December 12, 2021 (revised on 12/13/2021)

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

Customer managed Orchestrator and legacy GMS products are affected by this vulnerability. This includes on-premise and customer managed instances running in public cloud services such as AWS, Azure, Google, or Oracle Cloud. See **Corrective Action Required** for details about how to mitigate this exploit.

Unaffected Products

- EdgeConnect and Legacy NX, VX, VRX products do not use the Log4j2 library and are therefore not vulnerable.
- Silver Peak Hosted Cloud Orchestrator Services – Silver Peak Orchestrator as a Service (Orch-AAS), Orchestrator-SP, and Orchestrator Global Enterprise – are not affected. These services use AWS Shield as a WAF firewall in front of the service. AWS Shield blocks any attempts with code exploit strings.

Corrective Action Required

Customers running self-managed on-premise or cloud instances of Orchestrator or legacy GMS must take immediate action to prevent potential attackers from using this exploit. Follow the steps below to mitigate this exploit:

1. SSH to the Orchestrator virtual machine and log in as the **admin** user.
2. Change to the /home/gms/gms directory.
3. Open the file named "gmsserver" for editing.
4. Locate the line that starts with: exec $JAVA_HOME/bin/java
5. Add the text below just before com.silverpeak.gms.server.VistaPointServer

   -Dlog4j.formatMsgNoLookups=true

   Example before:

   ```
       exec $JAVA_HOME/bin/java --add-opens java.base/java.lang=ALL-UNNAMED -server -Xms256m -
   Xmx${Xmx}m -classpath ".:$BASE_DIR/properties:$BASE_DIR/metaData:$BASE_DIR/lib/*" -server -
   XX:ErrorFile=${HOME_DIR}/gms/logs/java_error%p.log -XX:HeapDumpPath=${HOME_DIR}/gms/logs -
   XX:+HeapDumpOnOutOfMemoryError ${JVM_ARGS} -Djdk.tls.ephemeralDHKeySize=2048 -
   Djava.io.tmpdir=${TEMP_DIR} -Djavax.net.ssl.trustStore=${HOME_DIR}/gms/properties/cacerts
   com.silverpeak.gms.server.VistaPointServer
   ```

   Example after:

   ```
       exec $JAVA_HOME/bin/java --add-opens java.base/java.lang=ALL-UNNAMED -server -Xms256m -
   Xmx${Xmx}m -classpath ".:$BASE_DIR/properties:$BASE_DIR/metaData:$BASE_DIR/lib/*" -server -
   XX:ErrorFile=${HOME_DIR}/gms/logs/java_error%p.log -XX:HeapDumpPath=${HOME_DIR}/gms/logs -
   XX:+HeapDumpOnOutOfMemoryError ${JVM_ARGS} -Djdk.tls.ephemeralDHKeySize=2048 -
   Djava.io.tmpdir=${TEMP_DIR} -Djavax.net.ssl.trustStore=${HOME_DIR}/gms/properties/cacerts
   -Dlog4j.formatMsgNoLookups=true com.silverpeak.gms.server.VistaPointServer
   ```

6. Save the file and reboot the Orchestrator virtual machine.
7. Test Orchestrator status from the browser to make sure Orchestrator is up and running.

   CAUTION: Any typo or error in editing the file may result in Orchestrator not starting. If this happens, repeat steps 1 through 6 to correct the mistake.

NOTE: For information about how to verify that the steps above are working, and for answers to common questions about this vulnerability, see the FAQ page.

Future Considerations

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

For any questions, please raise a technical support case with Silver Peak via Orchestrator, or online at https://www.silver-peak.com/.

Thank you,
Product Security Incident Response Team at Silver Peak