Silver Peak Security Advisory

Notification

Apache Log4j2 Vulnerability

Date: December 12, 2021 (revised on 01/04/2022)

CVE IDs: CVE 2021-44228, CVE-2021-45046, CVE 2021-45105, CVE-2021-44832

Summary

CVE 2021-44228: 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 protects against remote code execution by defaulting "com.sun.jndi.rmi.object.trustURLCodebase" and "com.sun.jndi.cosnaming.object.trustURLCodebase" to "false."

CVE 2021-45046: The fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 makes a best-effort attempt to restrict JNDI LDAP lookups to localhost by default. Log4j 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

CVE-2021-44832: Apache Log4j2 version 2.0 through 2.17.0 are vulnerable to a remote code execution (RCE) attack. The risk to Orchestrator is minimal as it requires SSH admin access to Orchestrator to modify /home/gms/gms/properties/log4j.xml. This is a low severity issue and will be addressed by upgrading your Orchestrator instance to an updated version containing Log4j 2.17.1. See the Apache Log4j FAQ for more information.

CVE 2021-45105: No Silver Peak products are affected by this vulnerability.

Affected Products

All Orchestrator and legacy GMS products are affected by CVE 2021-44228, CVE 2021-45046, and CVE-2021-44832, including:

- Self-managed on-premise Orchestrator
- Self-managed Orchestrator running in public cloud services
- Self-managed Cloud instances installed from marketplace images (AWS, Azure, GCP)
- Silver Peak Orchestrator as a Service (Orch-AAS)
- Orchestrator-SP and Orchestrator Global Enterprise – **tenants only**

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 not vulnerable.

Corrective Action Required for CVE 2021-44228, CVE 2021-45046, and CVE-2021-44832

- Customers running self-managed Orchestrator or legacy GMS (on-premise or cloud instances) must take **immediate action** to prevent potential attackers from using this exploit:
    - Manually patch the affected Orchestrator systems
    - Upgrade to a patched version of Orchestrator when available
- Customers using Silver Peak Orchestrator as a Service (Orch-AAS) should open a case with Silver Peak Support to have your managed cloud instances upgraded when possible.
- For customers using Orchestrator-SP or Orchestrator Global Enterprise, service providers must upgrade Orchestrator tenants when the upgrade is available.

NOTE: Details about specific actions to take as well as answers to common questions about this vulnerability and Silver Peak's response can be found in the Apache Log4j FAQ.

Future updates regarding this issue will be communicated via the FAQ page.

Thank you,
Product Security Incident Response Team at Silver Peak