Semarchy xDM Security Notice - Log4J - 2022-02

Engineering Team Response

Authors: FX Nicolas, Sebastien Arod, Arnaud Mergey, Rémi Aubel, Mehdi El Azrak, Nicolas Lenoire, Cédric Blanc
Updated: Feb 1, 2022

This document provides a status on the recent Common Vulnerabilities and Exposures (CVEs) reported on the Log4J library and provides responses from the Semarchy engineering team.

Contents

Overview

The Semarchy engineering team is constantly monitoring - as part of the build & quality processes - all Common Vulnerabilities and Exposures (CVEs) that impact libraries or third-party components shipped in the Semarchy products.

A vulnerability has been reported under the CVE-2021-44228 reference, affecting the Log4J2 (Log4J version 2) library, commonly used in applications for logging services.

To summarize:

- **CVE-2021-44228 impacts Log4J2 (Log4J version 2) until version 2.15, which is not used by any version of Semarchy xDM.**
- The logging in Semarchy xDM was upgraded from Log4J1 to Log4J2 as part of the 5.3.9 release (January 2022). The Log4J2 version (2.17.1) shipped with xDM 5.3.9 and above is **not vulnerable to CVE-2021-44228**.
- The Log4J2 version (2.17.1) shipped with xDM 5.3.9 and above is **not vulnerable either to the following CVEs** reported after CVE-2021-44228 and affecting earlier versions of Log4J2:
  - **CVE-2021-45046**
  - **CVE-2021-45105**
  - **CVE-2021-44832**
- xDM prior to version 5.3.9 uses Log4J1 (Log4J version 1) which is **not vulnerable** to CVE-2021-44228 attacks as described in the CVE.
- Log4J1 (one) has other reported vulnerabilities which can be easily identified and mitigated.

Do not hesitate to contact our support team if you have additional questions or need further clarifications.

CVE-2021-44228: Not Applicable/Low Risk

Description

Apache Log4J2 versions 2.0 to 2.14.1 (inclusive) are susceptible to a vulnerability which could allow an attacker who can control log messages or log message parameters to execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Semarchy Response

The Semarchy team has tested the most recent CVE-2021-44228 against xDM:

- From version 5.3.9, xDM uses Log4J 2.17.1 which is not concerned by CVE-2021-44228.
- We were **not** able to reproduce CVE-2021-44228 against the log4J1 version shipped with xDM versions prior to 5.3.9.
- We were only able to reproduce CVE-2021-44228 by replacing this Log4J version with the impacted Log4J2 version (2.15).

CVE-2021-44228 in Log4J2 (two) allows triggering an LDAP connection by means of log message.

Further investigations seem to indicate that Log4J1 (one) is *partially vulnerable* to CVE-2021-44228, under specific circumstances[1]:

- Reproducing this behavior in Log4J1 requires a user with Administrator privileges configuring a JMSAppender binding a topic name to trigger the LDAP connection, such as in the sample below.

```
log4j.appender.JMS = org.apache.log4j.net.JMSAppender
log4j.appender.JMS.InitialContextFactoryName =
org.apache.activemq.jndi.ActiveMQInitialContextFactory
log4j.appender.JMS.ProviderURL = tcp://localhost:61616
log4j.appender.JMS.TopicBindingName = ldap://127.0.0.1:1389/a
log4j.appender.JMS.TopicConnectionFactoryBindingName =
ConnectionFactory
```

- Since this second-level exploit requires administrative privileges, it is classified as **Low Risk** in the xDM platform for versions prior to 5.3.9 and **Not Applicable** from version 5.3.9.

[1] See https://github.com/apache/logging-log4j2/pull/608#issuecomment-991723301 for more details.

Other Log4J2 CVEs

The following CVEs were reported after CVE-2021-44228 and affect Log4J2 versions prior to 2.17.1.

CVE-2021-45046: Not Applicable

Description

The fix to address CVE-2021-44228 in Apache Log4J 2.15.0 was subject to a vulnerability that could allow an attacker in certain non-default configurations to craft malicious data using a JNDI Lookup pattern. Successful exploitation of this vulnerability could lead to disclosure of sensitive information, remote or local code execution.
Log4J 2.16.0 fixed this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

Semarchy Response

- Log4J 2.15.0 or earlier is not shipped with any version of Semarchy xDM.
- From version 5.3.9, xDM uses Log4J 2.17.1 which is not affected by CVE-2021-45046.

CVE-2021-45105: Not Applicable

Description

Apache Log4J2 until 2.16.0 did not protect from uncontrolled recursion from self-referential lookups. This vulnerability allows an attacker with control over Thread Context Map data to cause a Denial of Service when a crafted string is interpreted. This issue was fixed in Log4J 2.17.0.

Semarchy Response

- Log4J 2.16.0 or earlier is not shipped with any version of Semarchy xDM.
- From version 5.3.9, xDM uses Log4J 2.17.1 which is not affected by CVE-2021-45105.

CVE-2021-44832: Not Applicable

Description

Apache Log4J2 until 2.17.0 is vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed in Log4J2 2.17.1.

Semarchy Response

- Log4J 2.17.0 or earlier is not shipped with any version of Semarchy xDM.
- From version 5.3.9, xDM uses Log4J 2.17.1 which is not affected by CVE-2021-44832.

Other Log4J1 CVEs

The version of Log4J1 used in xDM prior to version 5.3.9 may be subject to other CVEs, listed below.

CVE-2019-17571: Not Applicable

Description

Included in Log4J 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4J versions 1.2 up to 1.2.17.

Semarchy Response

The Semarchy team is aware of CVE-2019-17571, identified against the Log4J version currently used in xDM. However, xDM does not use the component (the Log4J SocketServer is not started) involved in this security issue, and should not be vulnerable to these attacks.

CVE-2020-9488: Low Risk

Description

Improper validation of certificate with host mismatch in Apache Log4J SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.

Semarchy Response

The Semarchy team is aware of CVE-2020-9488, identified against the Log4J version currently used in xDM. This CVE may only affect instances configured with logging using an SMTP appender with SMTPS configured as the appender's `SMTPProtocol` property, as in the below example.

```
log4j.appender.sendMail = org.apache.log4j.net.SMTPAppender
log4j.appender.sendMail.SMTPHost = <smtp_host_name>
log4j.appender.sendMail.SMTPPort = <smtp_host_port>
log4j.appender.sendMail.SMTPProtocol=smtps
...
```

Mitigation

As a general rule, we do not recommend sending sensitive information or data for the purpose of integration via SMTP logging. SMTP logging is intended to raise issues to administrators who should authenticate to the xDM instance to take action.

If using the SMTP appender to transfer logs messages via email on unsecured networks, administrators should take action to mitigate this issue. To ensure the secure transfer of log messages via SMTP, administrators should follow the steps provided in the Log4J Issue: Set the system property `mail.smtps.ssl.checkserveridentity`[2] to `true` to globally enable hostname verification for SMTPS connections.

This can be done by setting this property in the java startup parameters, for example in the `setenv.sh|bat` file for a Tomcat Server.

```
CATALINA_OPTS="$CATALINA_OPTS -Dmail.smtps.ssl.checkserveridentity=true ...
```

CVE-2022-23302: Low Risk

Description

JMSSink in all versions of Log4J 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4J configuration or if the configuration references an LDAP

[2] See https://javaee.github.io/javamail/docs/api/com/sun/mail/smtp/package-summary.html

service the attacker has access to. This vulnerability can be exploited by an attacker to remotely execute arbitrary code.

Semarchy Response

This issue only affects Log4J 1.x which was replaced by Log4J2 in xDM version 5.3.9.
For xDM versions prior to 5.3.9:

- This CVE requires the JMSSink app to be specifically started, which is not the case in xDM.
- The Semarchy team recommends not using JMSSink and upgrading to xDM version 5.3.9.

CVE-2022-23305: Low Risk

Description

The JDBCAppender in Log4J 1.2 is vulnerable to SQL injection of untrusted data. This allows an attacker to execute unintended SQL queries on the server if the application is configured to use the JDBCAppender.

Semarchy Response

The Semarchy team is aware of CVE-2022-23305, identified against the Log4J version used by xDM prior to version 5.3.9. Instances running with xDM 5.3.9 and above are not affected by this vulnerability.
For xDM versions prior to 5.3.9, this CVE may only affect instances specifically configured to use the JBDCAppender for logging. Moreover, the appender should **never** be configured to connect to the target database with a user having extended privileges such as creating, dropping objects, or executing procedures.

Mitigation

The Semarchy team recommends not using the JDBCAppender for instances running with xDM versions prior to 5.3.9, and considering upgrading to version 5.3.9.
If using this appender with an affected version, administrators must configure it with a user having limited privileges and use this appender only for loggers that log static messages that do not include user inputs

CVE-2022-23307: Low Risk

Description

A deserialization issue was identified in Chainsaw, which was previously a component of Apache Log4J 1.2.x. This vulnerability allows an attacker to send a malicious request with serialized data that will be deserialized on the server when the Chainsaw component is run.

Semarchy Response

This issue only affects Log4J 1.x which was replaced by Log4J2 in xDM version 5.3.9.
For xDM versions prior to 5.3.9:

- This CVE requires the Chainsaw app to be specifically started, which is not the case in xDM.
- The Semarchy team recommends not using Chainsaw and upgrading to xDM version 5.3.9.

Further Questions

Do not hesitate to contact our support team if you have additional questions or need further clarifications.