Security Notice -Log4J - 2021-12

Engineering Team Response

Authors: FX Nicolas, Arnaud Mergey, Cyril Dussud, Ludovic Camus
Updated: Dec 14, 2021

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

Contents

Overview

The Semarchy/Stambia engineering team is monitoring - as part of the build & quality processes - Common Vulnerabilities and Exposures (CVEs) that impact libraries or third-party components shipped in the Semarchy/Stambia 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), which is not used in the Stambia Data Integration core components (Designer, Runtime and Analytics)**
  The Stambia core components use 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.
- The only component shipping Log4J2 (Log4J version 2) is the ElasticSearch component, which is not impacted by the CVE (it is a transitive dependency not exposed to end-user).

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/Stambia Response

Core Components: Designer, Analytics, Runtime

The engineering team has reviewed the most recent CVE-2021-44228 for Stambia Data Integration Core Components:

- Designer does not use Log4J for logging purposes.
- Runtime and Analytics do not use Log4J version 2, but use the previous version of that library, Log4J version 1, which is not affected directly by the CVE.

No core component in Stambia Data Integration is directly affected by this CVE.

CVE-2021-44228 in Log4j2 (two) allows triggering a 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 to configure a **JMSAppender** binding a topic name to trigger the LDAP connection.

Since this second-level exploit requires administrative privileges to configure a JMSAppender runtime logging, it is therefore classified as Low Risk in the Stambia Data Integration platform.

License Server

The License Server components include solely the API of Apache Log4j2 library and not the implementations. It is not subject to CVE-2021-44228.

Components & Connectors

The Apache Log4j2 library is included as a dependency in the Stambia ElasticSearch Connector, in a version that is affected by the CVE. However, the configuration of the logging in these connectors does not include an **LDAPAppender** required to exploit this CVE.

Other Log4J1 CVEs

The version of Log4J1 used in the Stambia Data Integration core components (Runtime and Analytics) may be subject to other CVEs, listed below.

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

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/Stambia Response

The engineering team is aware of CVE-2019-17571, identified against the Log4J version currently used in the Runtime and Analytics. However, these components do not use the feature (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/Stambia Response

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

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 their data integration systems 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 running Analytics.

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

Next Product Steps

Log4J version 2.x in ElasticSearch Component

Although not affected by this CVE, the ElasticSearch connector will be upgraded in the next connector release (3.0.0) to a most recent version of the Log4J2, including the fix for CVE-2021-44228.

Log4J version 2.x in License Server

Although not affected by this CVE, the License Server will be upgraded in the next release (5.3.0) to a most recent version of the Log4J2, including the fix for CVE-2021-44228.

Log4J version 1.x in Runtime and Analytics

The Log4J version 1.x library currently used in Stambia Data Integration Runtime and Analytics has reached end of life and applications using Log4j version 1.x are recommended to upgrade to Apache Log4j 2.x.

Upgrading the Log4J 1.x library to Log4J 2.x is a "technical debt" tracked as DI-2506. The change of library has an impact on the method used by administrators to configure the logging.

Due to the nature of this change, the product team planned to perform that upgrade as part of a next minor release (5.4). However, due to the growing number of issues raised on Log4J 1.x, the product team now considers performing this upgrade earlier with a smooth upgrade path.

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

Further Questions

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