Semarchy xDI Security Notice - Log4J - 2023-04

Engineering Team Response

Authors: FX Nicolas, Arnaud Mergey, Cyril Dussud, Ludovic Camus

Updated: Apr 24, 2023

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 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.

Multiple vulnerabilities affecting the **Log4J2 (Log4J version 2)** library, commonly used in applications for logging services, have been reported under the CVE-2021-44228, CVE-2021-45105, CVE-2021-44832, and CVE-2021-45046 references.

Multiple vulnerabilities affecting the **Log4J1 (Log4J version 1)** library, commonly used in applications for logging services, have been reported under the CVE-2019-17571, CVE-2020-9488, CVE-2022-23302, CVE-2022-23305, and CVE-2022-23307 references.

To summarize:

- The impact for each product is summarized below.
    - **Designer**
        - The Designer does not use Log4J for logging purposes. It is therefore **not affected** by the reported vulnerabilities.
    - **Analytics**
        - Analytics does not use Log4J2 (Log4J version 2). It is **not affected** by the Log4J2 (Log4J version 2) vulnerabilities.
        - Analytics uses the previous version of that library, Log4J1 (Log4J Version 1), which has other reported vulnerabilities. However, Analytics is **not affected** by these vulnerabilities.
        - **Although not affected**, Analytics has been upgraded in Semarchy xDI 2023.1.0 to use Log4J2 (Log4J version 2) 2.17.1 version.
    - **Runtime**
        - The Runtime does not use Log4J2 (Log4J version 2). It is **not affected** by the Log4J2 (Log4J version 2) vulnerabilities.
        - The Runtime uses the previous version of that library, Log4J1 (Log4J Version 1), which has other reported vulnerabilities that can be easily identified and **mitigated.**
        - The Runtime has been upgraded in Semarchy xDI 2023.1.0 to use Log4J2 (Log4J version 2) 2.17.1 version.
    - **Components**

        - The only component shipping Log4J2 (Log4J version 2) is the ElasticSearch component, which is **not affected** by the CVEs (it is a transitive dependency not exposed to end-users).
        - **Although not affected**, the ElasticSearch component **has been upgraded** in the Component Pack version 3.0.0 to use the Log4J2 (Log4J version 2) 2.16.0 version, which includes the fixes to CVE-2021-44228 and CVE-2021-45046.
        - **Although not affected**, the ElasticSearch component **has been upgraded** in the Component Pack version 3.0.2 to use the Log4J2 (Log4J version 2) 2.17.1 version, which includes the fix to CVE-2021-45105 and CVE-2021-44832
    - **License Server**
        - The License Server product includes solely the API of the Apache Log4J2 library and not the implementations. It is therefore **not affected** by the vulnerabilities.
        - **Although not affected**, the License Server **has been upgraded** in version 5.3.0 to use the Log4J2 (Log4J version 2) 2.16.0 version, which includes the fixes to CVE-2021-44228 and CVE-2021-45046.
        - **Although not affected**, the License Server **has been upgraded** in version 5.3.2 to use the Log4J2 (Log4J version 2) 2.17.1 version, which includes the fix to CVE-2021-45105 and CVE-2021-44832.

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

CVE-2021-44228 and CVE-2021-45046: Not Applicable/Low Risk

Description

Apache Log4J2 versions 2.0.x to 2.15.0 (inclusive) are susceptible to a vulnerability that 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 the disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Semarchy/Stambia Response

The engineering team has reviewed the most recent CVE-2021-44228 and CVE-2021-45046 for Stambia Data Integration/Semarchy xDI core products and components.

No products in Stambia Data Integration/Semarchy xDI are directly affected by these CVEs:

- Designer
  - The Designer does not use Log4J for logging purposes. It is therefore **not affected** by the reported vulnerabilities.
- Analytics
  - Analytics does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** directly by these CVEs.
- Runtime
  - The Runtime does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** directly by these CVEs.
- Components
  - The Apache Log4J2 library was included as a dependency in the ElasticSearch Connector, in a version that is affected by these CVEs. However, the configuration of the logging in this connector does not include an **LDAPAppender** required to exploit this CVE, and the configuration is not exposed and not modifiable. The component is therefore **not affected** by these CVEs.
  - **Although not affected**, the ElasticSearch component **has been upgraded** in version 3.0.0 to use the Log4J2 (Log4J version 2) 2.16.0 version, which includes the fix to CVE-2021-44228 and CVE-2021-45046.
- License Server

- The License Server components include solely the API of the Apache Log4J2 library and not the implementations. It is **not affected** by these CVEs.
- **Although not affected**, the License Server **has been upgraded** in version 5.3.0 to use the Log4J2 (Log4J version 2) 2.16.0 version, which includes the fix to CVE-2021-44228 and CVE-2021-45046.

CVE-2021-44228 in Log4J2 (Log4J version 2) 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 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/Semarchy xDI platform.

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

CVE-2021-45105: Not Applicable

Description

Apache Log4J2 versions 2.0-alpha1 through 2.16.0 (inclusive) (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted.

Semarchy/Stambia Response

The engineering team has reviewed the CVE-2021-45105 for Stambia Data Integration/Semarchy xDI core products and components.

No products in Stambia Data Integration/Semarchy xDI are affected by this CVE:

- Designer
  - The Designer does not use Log4J for logging purposes. It is therefore **not affected** by the reported vulnerabilities.
- Analytics
  - Analytics does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** by the CVE.
- Runtime
  - The Runtime does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** by the CVE.
- Components
  - The Apache Log4J2 library was included as a dependency in the ElasticSearch component, in a version that is affected by the CVE. However, exploiting the vulnerability requires accessing the Log4J2 (Log4J version 2) configuration, which is not exposed by the Elasticsearch component and is not modifiable. The component is therefore **not affected** by the CVE.
- License Server
  - The License Server components include solely the API of the Apache Log4J2 library and not the implementations. It is **not affected** by this CVE.

CVE-2021-44832: Not Applicable

Description

Apache Log4J2 versions 2.0-beta7 through 2.17.0 (inclusive) (excluding security fix releases 2.3.2 and 2.12.4) are 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.

Semarchy/Stambia Response

The engineering team has reviewed the CVE-2021-44832 for Stambia Data Integration/Semarchy xDI core products and components.

No products in Stambia Data Integration/Semarchy xDI are affected by this CVE:

- Designer
  - The Designer does not use Log4J for logging purposes. It is therefore **not affected** by the CVE.
- Analytics
  - Analytics does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** by the CVE.
- Runtime
  - The Runtime does not use Log4J2 (Log4J version 2) but uses the previous version of that library, Log4J version 1, which is **not affected** by the CVE.
- Components
  - The Apache Log4J2 library was included as a dependency in the ElasticSearch component, in a version that is affected by the CVE. However, exploiting the vulnerability requires accessing the Log4J2 (Log4J version 2) configuration, which is not exposed by the Elasticsearch component and is not modifiable. The component is therefore **not affected** by the CVE.
- License Server
  - The License Server components include solely the API of the Apache Log4J2 library and not the implementations. It is **not affected** by this CVE.

Other Log4J1 CVEs

The version of Log4J1 used in the Stambia Data Integration/Semarchy xDI core components (Runtime and Analytics) 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/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 products 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 ...
```

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

Semarchy Response

The engineering team is aware of CVE-2022-23302, identified against the Log4J version currently used in the Runtime and Analytics.

This CVE requires the JMSSink app to be specifically started and a physical access and permission to provide a malicious configuration.

- Analytics does NOT start the JMSSink app and is therefore **not affected** by this CVE. Moreover, Analytics does not expose the Log4J1 (Log4J Version 1) configuration file.
- The Runtime does NOT start the JMSSink app, and is therefore **not directly affected** by this CVE. However, it exposes the Log4J1 (Log4J Version 1) configuration file and therefore **may be affected** if a user provides a malicious configuration. This requires permission to access and modify the configuration file, which can be easily **mitigated**.

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

Mitigation

This CVE requires the JMSSink app to be started, which is not the case in Analytics and in the Runtime by default. The Semarchy team recommends not using JMSSink.

Exploiting the vulnerability requires permission to access and modify the runtime configuration file to enable JMSSink. As a general rule, we recommend securing the access and the edition of the Runtime files. Only administrators and dedicated users with dedicated permissions should be able to access and modify the Runtime files and configuration.

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 engineering team is aware of CVE-2022-23305, identified against the Log4J version currently used in the Runtime and Analytics.

This CVE may only affect instances specifically configured to use the JBDCAppender for logging.

- Analytics is not using the JDBCAppender and does not expose the Log4J1 (Log4J Version 1) configuration file. Although it uses Log4J1 (Log4J Version 1), Analytics is therefore **not affected** by this CVE.
- The Runtime, with a default configuration, is not using the JDBCAppender, and is therefore **not directly affected** by this CVE. However, it exposes the Log4J1 (Log4J Version 1) configuration file and therefore **may be affected** if a user defines a JDBCAppender inside. This requires permission to access and modify the configuration file, which can be **easily mitigated**.

Mitigation

The Semarchy team recommends not configuring a JDBCAppender for the logging of the Runtime.

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.
As a general rule, we recommend securing the access and the edition of the Runtime files. Only administrators and dedicated users with dedicated permissions should be able to access and modify the Runtime files and configuration.

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

The engineering team is aware of CVE-2022-23307, identified against the Log4J version currently used in the Runtime and Analytics.

This CVE requires the Chainsaw app to be specifically started and used, which is not the case in the Runtime and Analytics, which are therefore **not affected directly** by this CVE.

This CVE affects only the users that use Chainsaw, which is a GUI log viewer, to consult the logs of the Runtime or Analytics. Chiansaw is not shipped with xDI and the Semarchy team recommends not using Chainsaw.

Further Questions

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