Software AG Security Advisory

Apache Log4j (Log4Shell) Vulnerabilities

Announced: Jan-2022

Affects: There are multiple vulnerabilities associated with log4j library which got unfolded from early December till the end of the month. Many of the java-based products of Software AG are impacted by the log4j vulnerabilities. The precise list is provided in the 'Impact' section of this document.

Severity: Critical

I. Description

Apache Log4j is an open-source Java logging library developed by the Apache Foundation which is widely used in many enterprise applications including Software AG products.

On December 9, 2021, security researchers discovered a flaw in the code of a software library used for logging. The flaw was rated a 10 out of 10 on the Common Vulnerability Scoring System, or CVSS, due to the potential impact that it can have if leveraged by attackers. Details of the vulnerability can be found in the National Vulnerability Database (NVD) under the heading CVE-2021-44228.

As of Dec. 14, researchers discovered that the fix developed for CVE-2021-44228 was incomplete and the vendor, Apache, released a new fix. On Dec. 17, two new issues were confirmed and the next day, Apache released another fix.

To simplify things, the current list of vulnerabilities and recommended fixes are listed here:

- CVE-2021-44228 (CVSS score: 10.0) - A remote code execution vulnerability affecting Log4j versions from 2.0-beta9 to 2.14.1 (Fixed in version 2.15.0)
- CVE-2021-45046 (CVSS score: 9.0) - An information leak and remote code execution vulnerability affecting Log4j versions from 2.0-beta9 to 2.15.0, excluding 2.12.2 (Fixed in version 2.16.0)
- CVE-2021-45105 (CVSS score: 5.9) - A denial-of-service vulnerability affecting Log4j versions from 2.0-beta9 to 2.16.0 (Fixed in version 2.17.0)
- CVE-2021-4104 (CVSS score: 8.1) - An untrusted deserialization flaw affecting Log4j version 1.2 (No fix available; Upgrade to version 2.17.0)
- CVE-2021-44832 (CVSS score: 6.6) - Remote code execution vulnerability affecting Log4j2 versions 2.0-beta7 through 2.17.0, excluding security fixes for 2.3.2 and 2.12.4. (Fixed by upgrading to 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later).

As soon as the vulnerability information was leaked our security team and product teams proactively worked to release the mitigation/ workaround steps for each product to curb the vulnerability as well as started the work for official fixes. Refer to the 'Workaround' and 'Fix' section for relevant information impacted product wise. Also, refer to the Log4Shell Customer Security FAQ for frequently asked questions.

Note: This document will be updated if there are more updates or vulnerabilities released related to log4j library.

Reference:

https://logging.apache.org/log4j/2.x/security.html

https://www.cisecurity.org/log4j-zero-day-vulnerability-response/

https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

II. Impact

There are multiple vulnerabilities identified in Log4j library which leads to various attacks including Remote code execution (RCE), Information leakage etc.

The impact to Software AG products depends on the usage and configuration. When not patched, the JNDI features used in configurations, 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.

A similar attack might occur when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $${ctx:loginId}), attackers with control over Thread Context Map (MDC) input data can craft malicious input data using a JNDI Lookup pattern. This leads to information leak and/ or remote code execution in some environments.

There is no known impact identified in Software AG products for StackOverflow exception and RCE via JDBC Appender. However, the fixes for latest Log4j version are in progress. Refer to the 'Fixes' section of this document for more information.

III. Workaround/Mitigating Factors

Mitigation steps for impacted products are listed in the Knowledge Base (KB) articles for each impacted product line. Refer to the KB articles given below for detailed steps. Please note that you will need your Empower credentials to access the following links.

- Adabas
- ARIS Connect/Design-Server On-Premise
- ARIS Cloud Enterprise
- ARIS Process Performance Manager
- ConnX
- Cumulocity IoT On-Premise (including Edge, Apama, DataHub, Zementis)
- Cumulocity IoT Cloud (including Apama, DataHub, Zementis)
- MashZone
- MashZone NG
- Natural
- webMethods - Multiple Products
- webMethods ApplinX
- webMethods EntireX
- webMethods JIS/JI

IV. Fixes for the affected versions

The information about the affected version can be found in the KB article mentioned in the **Workaround/Mitigating Factors** section.

The necessary information about the fixes can be seen in the Product Fixes section in Empower https://empower.softwareag.com/KnowledgeCenter/Product_Fixes/default.aspx

To get the Early warning updates please subscribe to it in Empower – https://empower.softwareag.com/Preferences/ManageMySubscriptions/earlywarnings.aspx

V. Contacting Us

If you have questions about this alert or need to report an additional issue, do send an email to Software AG security team:

email : [security@softwareag.com|mailto:security@softwareag.com]

You can reach authorized technical support contacts can reach Software AG Global Support in the following ways:

Web : https://empower.softwareag.com/eservice/default.aspx (deprecated - online support centre)

Or https://getsupport.softwareag.com/ (new – support portal)

You can find the complete contact information in our Global Support Contact Directory at

https://empower.softwareag.com/public_directory.aspx

You can also participate in our Software AG Developer Communities, which feature technical information, useful resources, and online discussion forums, moderated by Software AG professionals, to help you do more with technology:

http://www.softwareag.com/Corporate/community/dev_net/default.asp

VI. Copyright

Copyright (c) 2022 by Software AG. Permission is granted for copying and circulating this bulletin to Software AG customers for the purpose of alerting them to those topics covered by this bulletin, if and only if, this bulletin is not edited or changed in any way, is attributed

to Software AG and provided such reproduction and/or distribution is performed for non-commercial purposes. Any other use of this information is prohibited.