Security Advisory
Apache Log4j Vulnerabilities

1 Advisory Information

Advisory ID: BOSCH-SA-572602
CVE Numbers and CVSS v3.1 Scores:

- CVE-2021-44228
  - Base Score: 10.0 (Critical)
- CVE-2021-44832
  - Base Score: 6.6 (Medium)
- CVE-2021-45046
  - Base Score: 9.0 (Critical)
- CVE-2021-45105
  - Base Score: 7.5 (High)

Published: 21 Dec 2021
Last Updated: 10 Jan 2022

2 Summary

The Apache Software Foundation has published information about a vulnerability in the Java logging framework *log4j*, which allows an attacker to execute arbitrary code loaded from LDAP or JNDI related endpoints which are under control of the attacker. [1]
Additionally, a further vulnerability might allow an attacker to cause a denial of service by sending a crafted string to the framework.
From Bosch Rexroth, only the IoT Gateway software has been identified as affected.
This document is updated in case new information arises regarding other products.

3 Affected Products

- IoT Gateway for Windows 2.1.0 – 2.3.2 (based on mbs OSGi)
- IoT Gateway for Windows 2.0.1 – 3.1.0 (based on Felix OSGi)
- IoT Gateway for Ubuntu Core 2.1.0 – 2.3.2 (PR21 Hardware)

4 Solution

4.1 Update to latest IoT Gateway version

Only the above-mentioned versions are affected. It is strongly advised to update to a non-affected IoT Gateway version, preferably the latest version (currently 3.7.0). To verify whether your installation is affected, check the version that is used. When updating from 2.1.x, existing configurations must be transferred using the Backup / Restore bundle and manual interaction is required before restoration.

Please contact your sales partner or the Bosch Rexroth support in case you need further assistance.

4.2 Compensatory Measures

When the IoT Gateway is operated in a segmented, isolated network the potential risk of an attacker being able to exploit the vulnerability can be reduced. Such compensatory measures are to be defined individually in the context of the operational environment. The “Security Guideline Electric Drives and Controls” [2] provides assistance regarding potential measures.

Please note that due to the high severity rating of the vulnerability, it is strongly advised to use an up-to-date version of the IoT Gateway software which is not affected instead of implementing compensatory measures.

5 Vulnerability Details

5.1 CVE-2021-44228

CVE description: Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 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. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

- Problem Type:
  - CWE-502 Deserialization of Untrusted Data
  - CWE-400 Uncontrolled Resource Consumption
  - CWE-20 Improper Input Validation
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 10.0 (Critical)

5.2 CVE-2021-44832

CVE description: Apache Log4j2 versions 2.0-beta7 through 2.17.0 (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. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

- Problem Type:
  - CWE-20 Improper Input Validation
  - CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component (‘Injection’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 6.6 (Medium)

5.3 CVE-2021-45046

CVE description: It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows 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.

- Problem Type:
  - CWE-502 Deserialization of Untrusted Data
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 9.0 (Critical)

5.4 CVE-2021-45105

CVE description: Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) 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. This issue was fixed in Log4j 2.17.0 and 2.12.3.

- Problem Type:
  - CWE-20 Improper Input Validation
  - CWE-674: Uncontrolled Recursion
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

6 Additional Resources

[1] Apache Log4j Security Vulnerabilities:
https://logging.apache.org/log4j/2.x/security.html
[2] Security Guideline Electric Drives and Controls:
https://www.boschrexroth.com/de/de/myrexroth/media-directory-download?object_nr=R911342562

7 Revision History

10 Jan 2022: Add CVE-2021-44832
21 Dec 2021: Initial Publication