Log4j Vulnerabilities - Impact on PRAESENSA Advanced Public Address Server (PRA-APAS)

BOSCH-SA-993110-BT

1 Advisory Information

- **Advisory ID:** BOSCH-SA-993110-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-44228
    - Base Score: 10.0 (Critical)
  - CVE-2021-45046
    - Base Score: 9.0 (Critical)
  - CVE-2021-45105
    - Base Score: 7.5 (High)
- **Published:** 22 Dec 2021
- **Last Updated:** 22 Dec 2021

2 Summary

The 1.0.31 software version of the PRAESENSA Advanced Public Address Server (PRA-APAS) contains version 2.10.0 of the Apache Log4j logging service. Recently Apache has warned that this Log4j version contains multiple vulnerabilities, including the Log4Shell vulnerability (CVE-2021-44228).

This Log4Shell vulnerability allows remote code execution by sending a specifically crafted log command to the PRA-APAS under certain conditions. This extremely critical vulnerability affects many products globally and is currently being actively exploited.

3 Affected Products

- Bosch PRA-APAS
  - CVE-2021-45105
- Bosch PRA-APAS < 1.0.32
  - CVE-2021-44228
  - CVE-2021-45046

4 Solution and Mitigations

4.1 Solution

Upgrade the PRA-APAS firmware to version 1.0.32 (PRAESENSA downloads)

- Version 1.0.32 upgrades Log4j to version 2.16.0 which removes all currently known Remote Code Execution vulnerabilities (CVE-2021-44228 but also CVE-2021-45046 which was uncovered in version 2.15.0)

Instructions on how to update can be found in chapter 5.4 of the configuration manual. The configuration manual (PRA-APAS V1.00) can be downloaded here: Advanced Public Address Server

Apache has released version 2.17.0 of Log4j since it was found that version 2.16.0 contains a Denial Of Service vulnerability (CVE-2021-45105). Since Bosch believes that the highest priority is to close the Remote Code Execution vulnerabilities first and since integration and testing of the 2.16.0 version had already started when 2.17.0 was released the 1.0.32 version is still made available first. A next version which will upgrade Log4j to version 2.17.0 (or newer) will follow later on. Due to that it is advised to check and implement the mitigation steps below.

4.2 Mitigation 1

All CVEs:

Isolate the PRA-APAS from the Internet and place it behind a firewall to make sure that it is no longer accessible. This can be done by placing the PRA-APAS behind a firewall or disabling the port-forwarding in the existing firewall.

CVE-2021-44228 (Log4Shell) and CVE-2021-45056:

Block PRA-APAS from accessing all internet access by configuring the firewall accordingly. Note that this second step is not needed if the PRA-APAS is updated to version 1.0.32.

4.3 Mitigation 2

All CVEs:

Use strong login credentials for the PRA-APAS, i.e. use strong passwords for the PRA-APAS. Using strong credentials already reduces the risk significantly of being hacked since the logging service can only be used by authorized users.

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-2021-45046

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 an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix 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)

5.3 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)

5.4 Remark

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

6 Additional Resources

- [1] Software Download Catalog: https://licensing.boschsecurity.com/publicaddress
- [2] Apache Log4j Security Vulnerabilities: https://logging.apache.org/log4j/2.x/security.html

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

7 Revision History

- 22 Dec 2021: Initial Publication

8 Appendix

8.1 Material List

Please find the SAP Number and CTN below.

SAP Number	CTN
F.01U.354.303	PRA-APAS