PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Notice #15/2021

Log4Shell - Impact on B&R Products

Document Version: 1.1

First published: 2021-12-15
Last updated: 2022-03-08

Executive Summary

On December 9th, 2021, a vulnerability was disclosed in Apache Log4j2 with CVE-2021-44228 [1]. B&R is aware of this security issue, known as `Log4Shell`.

During further investigations, an issue was also discovered in the Log4j 1.x. This vulnerability is tracked as CVE-2021-4104 [2].

Another Log4j 1.x security issue was publicly disclosed in January 2022 under CVE-2022-23307. B&R Cyber Security for Products addressed this vulnerability in its Security Advisory "A flaw in Chainsaw component of Log4j can lead to code execution" [3].

B&R has concluded the impact analysis for all potentially affected B&R products.

Affected Products

No products of B&R have been identified as affected by CVE-2021-44228 (`Log4Shell`).

APROL uses Log4j 1.x versions which are affected by CVE-2021-4104.
With the default configuration shipped with APROL this vulnerability cannot be exploited.
Using APROL provided tools and mechanisms, a CVE-2021-4104 vulnerable APROL system cannot be configured.

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines.
Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

References

[1] CVE-2021-44228 Details in the National Vulnerability Database

`https://nvd.nist.gov/vuln/detail/CVE-2021-44228`

[2] CVE-2021-4104 Details on MITRE

`https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104`

[3] B&R Advisory: A flaw in Chainsaw component of Log4j can lead to code execution

`https://www.br-automation.com/downloads_br_productcatalogue/assets/1644947115875-en-original-1.0.pdf`

Document History

Version	Date	Description
1.0	2021-12-15	Initial version
1.1	2022-03-08	Referenced related Log4j Security Advisory Updated impact analysis status