Cyber Security Advisory #02/2022

A flaw in Chainsaw component of Log4j can lead to code execution

Document Version: 1.0

First published: 2022-03-03
Last updated: N/A (Initial version)

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from B&R, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Executive Summary

CVE-2022-23307 A flaw in Chainsaw component of Log4j can lead to code execution
The deserialization issue in the Apache Chainsaw <2.1.0 component of Apache Log4j 1.x, shipped with B&R APROL AutoYaST <=V4.2-064.0.211004, Apache Directory Studio (via APROL AutoYaST) <=V4.2-064.0.211004, Squirrel-sql <=3.9.0, JSignPDF <=1.6.4, Jaspersoft JasperReports-Server <=7.1.3, and Jaspersoft Jaspersoft Studio Pro <=7.1.0 may allow an unauthenticated network-based attacker to execute code on affected installations.

Affected Products

Affected products: B&R APROL and B&R APROL installed third-party software components

Software product	Affected Versions	Patched Version	Patch availability
B&R APROL AutoYaST	<=V4.2-064.0.211004	V4.2-064.0.220131	2022-02-10
Apache Directory Studio (via APROL AutoYaST)	<=V4.2-064.0.211004	via APROL AutoYaST V4.2-064.0.220131	2022-02-10
Squirrel-sql	<=3.9.0	via APROL AutoYaST V4.2-064.0.220131	2022-02-10
JSignPDF	<=1.6.4	2.1.0 via APROL R4.2-06 P8	Planned: Q2 2022
JasperReports-Server	<=7.1.3	7.9.1	Planned: Q3 2022
Jaspersoft Studio Pro	<=7.1.0	Fix planned	Planned: Q3 2022

Table 1: Overview on affected, patched versions and release dates

The time period in Table 1 denoted as planned is preliminary and may be subject to change.

Vulnerability ID

CVE-2022-23307 A flaw in Chainsaw component of Log4j can lead to code execution

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.

CVE-2022-23307 A flaw in Chainsaw component of Log4j can lead to code execution

CVSS v3 Base Score:	9.8 (Critical)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Corrective Actions or Resolution

The described vulnerabilities will be fixed in the product versions as listed in Table 1.
Information about the availability of patches will be updated.

B&R recommends applying product updates at the earliest convenience, as well as implementing the actions listed in the section "Workarounds and Mitigations".

Vulnerability Details

CVE-2022-23307 A flaw in Chainsaw component of Log4j can lead to code execution

Description

The third-party Apache Chainsaw software component versions <2.1.0 are affected by a deserialization issue[2], which is part of the third-party Apache Log4j software component versions 1.x.
Affected Apache Log4j versions are included in impacted B&R APROL installations.

The vulnerability affects different components within impacted B&R APROL installations:

- B&R APROL and Apache Directory Studio via the operating system wide installed Log4j software component
- Squirrel-sql, JSignPDF, JasperReports-Server, and Jaspersoft Studio Pro via individually bundled Log4j software components

The impacted software component details are listed in Table 1.

Impact

An attacker could leverage this vulnerability to potentially execute code within the context of the affected software component, which might threaten the integrity and confidentiality of data or may cause a denial of service.

Fix

B&R APROL
A vendor patched; non-affected version is being installed via the APROL AutoYaST update.

Apache Directory Studio
This third-party software component is being updated to a vendor patched; non-affected version via the APROL AutoYaST update.

Squirrel-sql
This third-party software component is being removed via the APROL AutoYaST update.

JSignPDF
This third-party software component is being updated to a vendor patched; non-affected version via the APROL AutoYaST update.

Jaspersoft JasperReports-Server and Jaspersoft Studio Pro
This third-party software component is being updated to a vendor patched; non-affected version via the APROL AutoYaST update.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.

B&R APROL

For B&R APROL itself, the vulnerability is not exploitable in default installations.

B&R APROL Third-Party Software Components

The following affected third-party software components, shipping with impacted B&R APROL installations address specific customer use cases. Depending on the customer use case, these software components may be removed to fully mitigate the vulnerability.
The software removal is documented via APROL Support. Additionally, the APROL R4.2 D6 Security Documentation[1] should be consulted for enhancing the Cyber Security posture of APROL installations.

Apache Directory Studio

This auxiliary software component for managing LDAP server offers client-side network connectivity.

B&R recommends restricting user access to APROL installations.

Squirrel-sql

This auxiliary software component offers database connection debugging using client-side network connectivity.

B&R recommends limiting network communication to legitimate network communication partners, e.g. by setting up fine-grained firewall rules.

JSignPDF

This auxiliary software component for digitally signing PDF documents does not offer network connectivity.

B&R recommends restricting user access to APROL installations.
Additionally, it should be verified only authorized users may be able to perform signing operations. This APROL permission configuration is documented via APROL Support.

Jaspersoft JasperReports-Server and Jaspersoft Studio Pro

This auxiliary software component is used to configure and generate reports.

This software component opens on default the TCP listening ports 8080 and 8443 on all network interfaces.
B&R recommends configuring the APROL firewall to restrict access to the JasperReports-Server component for only authorized communication partners.
Additionally, B&R recommends limiting access to authorized users.

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] APROL R4.2 D6 Security Documentation

`https://www.br-automation.com/en/downloads/software/aprol-process-control/r-42-06/documentation/aprol-r42-d6-security-3/`

[2] MITRE entry on CVE-2022-23307

`https://nvd.nist.gov/vuln/detail/CVE-2022-23307`

Document History

Version	Date	Description
1.0	2022-03-03	Initial version