Cyber Security Advisory #11/2021

Zip Slip Vulnerability in B&R Automation Studio Project Import

Document Version: 1.0

First published: 2021-10-29
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-2021-22281 Zip Slip Vulnerability in B&R Automation Studio Project Import
A directory traversal vulnerability in the handling of project files in B&R Automation Studio >=4.0 versions allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.

Affected Products

All versions of Automation Studio 4 are affected.

Vulnerability ID

CVE-2021-22281 Zip Slip Vulnerability in B&R Automation Studio Project Import

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2021-22281 Zip Slip Vulnerability in B&R Automation Studio Project Import

CVSS v3.1 Base Score:	6.3 (Medium)
CVSS v3.1 Vector:	V:L/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N

Corrective Actions or Resolution

B&R recommends implementing the actions listed in the section “Workaround and Mitigations”.

Vulnerability Details

CVE-2021-22281 Zip Slip Vulnerability in B&R Automation Studio Project Import

Description

Attacker could use crafted B&R Automation Studio project files holding directory traversal filenames to trigger this vulnerability. By opening such a project in B&R Automation Studio, files may be added or changed on the local file system, using the privileges of the B&R Automation Studio user.

Impact

An attacker could leverage this vulnerability to potentially change or add data on the target system.

Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations:

Open only B&R Automation Studio project files from trusted source.
Use encrypted export of B&R Automation Studio project files, thus only allowing access to legitimate users.
Protect locations where B&R Automation Studio projects are stored from unauthorized access. This includes PLCs, when using the feature to back up project source files on target.
Do not run B&R Automation Studio in elevated mode.
Make sure, that Windows User Access Control (UAC) is enabled.
Verify integrity of B&R Automation Studio project files, which are exchanged via potentially insecure channels

In general, B&R recommends implementing the Cyber Security guidelines.

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/

Acknowledgements

B&R would like to thank the following for working with us to help protect our customers:
Mr. Mashav Sapir of Claroty
Mr. Andrew Hofmans

Document History

Version	Date	Description
1.0	2021-10-29	Initial version