PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #12/2021

RCE Vulnerability in B&R Automation Studio

Document Version: 1.0

First published: 2021-10-29
Last updated: N/A (Initial version)

Notice

Executive Summary

CVE-2021-22282 Remote Code Execution with crafted project files
Improper copy algorithm in the project extraction component in B&R Automation Studio version >=4.0 may allow an unauthenticated attacker to execute code.

Affected Products

All versions of Automation Studio 4 are affected.

Vulnerability ID

Vulnerability Severity

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

CVSS v3.1 Base Score:	8.3 (High)
CVSS v3.1 Vector:	AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Corrective Actions or Resolution

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

Vulnerability Details

Description

There is a file handling issue in the project extraction algorithm of B&R Automation Studio. The algorithm may enable adversaries link forged files instead of B&R provided ones. Successful exploitation of these vulnerability will enable the attacker to perform a code execution with the privileges of the application, when opening a specially crafted B&R Automation Studio project.

Impact

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

Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations:

Open only B&R Automation Studio project files from trusted source.
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.
Verify integrity of B&R Automation Studio project files, which are exchanged via potentially insecure channels.
Make sure, that Windows User Access Control (UAC) is enabled.

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