PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #01/2022

RCE through Project Upload from Target (“Evil PLC Attack”)

Document Version: 1.2

First published: 2022-01-20
Last updated: 2022-08-16

Executive Summary

CVE-2021-22289 RCE through Project Upload from Target
Improper copy algorithm and component validation in the project upload mechanism in B&R Automation Studio version >=4.0 may allow an unauthenticated attacker to execute code. Based on this vulnerability, an attack vector called “Evil PLC Attack” has been disclosed [1].

Affected Products

All versions of Automation Studio 4 are affected.

Vulnerability ID

CVE-2021-22289 RCE through Project Upload from Target

Vulnerability Severity

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

CVE-2021-22289 RCE through Project Upload from Target

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

CVE-2021-22289 RCE through Project Upload from Target

Description

If the PLC has not been sufficiently secured, an attacker could manipulate the stored project information. Alternatively, a remote attacker may use spoofing techniques to make B&R Automation Studio connect to an attacker-controlled device with manipulated project files. When using project upload in B&R Automation Studio, such crafted projects will be loaded and opened in the security context of Automation Studio. This may result in remote code execution, information disclosure and denial of service of the system running B&R Automation Studio.

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

The feature is not activated by default. Do not use the feature if it is not necessary for the project.

If the feature is activated, B&R recommends the following additional measures:

Use only ANSL over SSL and enable authentication on the PLC.
Always configure password protection when using the feature “Backing up project source files on the target system”. Use strong passwords.
Protect networks with PLCs from unauthorized access for example by using firewalls.
Do not run B&R Automation Studio with elevated user privileges.
Verify integrity of B&R Automation Studio project files, which are exchanged via potentially insecure channels, e. g. using hashes or digital signatures.
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

References

[1] Claroty's publication about Evil PLC Attack: Weaponizing PLCs

https://claroty.com/team82/research/white-papers/evil-plc-attack-weaponizing-plcs

Document History

Version	Date	Description
1.0	2022-01-20	Initial version
1.1	2022-01-20	Corrected CVE number
1.2	2022-08-16	Added refence to "Evil PLC Attack"