Cyber Security Advisory #10/2021

DLL Hijacking Vulnerability in Automation Studio

Document Version: 1.1

First published: 2021-10-29
Last updated: 2024-05-14

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-2021-22280 DLL Hijacking Vulnerability in Automation Studio
Improper DLL loading algorithms in B&R Automation Studio may allow an authenticated local attacker to execute code with elevated privileges.

Affected Products

Automation Studio <4.12

Vulnerability ID

CVE-2021-22280 DLL Hijacking Vulnerability in Automation Studio

Vulnerability Severity

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

CVE-2021-22280 DLL Hijacking Vulnerability in Automation Studio

CVSS v3.1 Base Score:	7.2 (High)
CVSS v3.1 Vector:	AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

Corrective Actions or Resolution

The described vulnerability is fixed in Automation Studio version 4.12 and higher. B&R advises customers to update to a patched version of Automation Studio.

Vulnerability Details

CVE-2021-22280 DLL Hijacking Vulnerability in Automation Studio

Description

A vulnerability exists in B&R Automation Studio that could allow an authenticated, local attacker to load a malicious DLL. Both local access and authentication are required to successfully exploit this vulnerability. This means that the potential attacker must have valid credentials and access to the system.
If exploited the attacker could place a malicious DLL file on the target system that, when running B&R Automation Studio could allow the attacker to execute arbitrary code with the privileges of another user's account.

Impact

An attacker could leverage this vulnerability to potentially elevate his privileges, which might threaten the integrity and confidentiality of data or cause a denial of service.

Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations:

- Restrict access to the installation directory of B&R Automation Studio to authorized users.
- Do not use multiple user accounts on computers with B&R Automation Studio installation.
- Make sure, that all installed assemblies are signed with valid B&R certificates.
- 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
1.1	2024-05-14	Updated information about the fixed version