



## Cyber Security Advisory #08/2021

### Denial of service vulnerability on Automation Runtime webserver

Document Version: 1.0

First published: 2021-07-09

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-2021-22275 Denial of service vulnerability on Automation Runtime webserver  
Improper buffer restrictions in the webserver of Automation Runtime versions prior to 4.91 may allow an unauthenticated network-based attacker to stop the cyclic program on the device and cause a denial of service.

## Affected Products

Affected versions: Please refer to Table 1

Affected Base Versions	Patched Version	Patch Availability
All versions prior to 4.7x	-	-
4.7x	D4.73	April 2021
4.8x	C4.83	May 2021
4.90	D4.90	April 2021

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

Automation Runtime version 4.91 and higher are **not affected**.

## Vulnerability ID

CVE-2021-22275 Denial of service vulnerability on Automation Runtime webserver

## Vulnerability Severity

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

CVE-2021-22275 Denial of service vulnerability on Automation Runtime webserver

CVSS v3.1 Base Score: 8,6 (High)

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

## Corrective Actions or Resolution

The described vulnerabilities have been fixed in the product versions as listed in Table 1.

B&R recommends applying product updates at the earliest convenience.



## Vulnerability Details

### CVE-2021-22275 Denial of service vulnerability on Automation Runtime webserver

#### Description

The webserver component of B&R Automation Runtime implements insufficient checks on handling file uploads. This implementation could result in a memory violation, which in turn affects the stability of Automation Runtime.

#### Impact

An attacker could leverage this vulnerability to potentially cause a denial of service of the device.

#### Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations:  
The access to the Automation Runtime webserver should be restricted to legitimate network partners, using e.g. a sufficient Firewall setup and robust network segmentation.  
B&R recommends deactivating Automation Runtime webserver when not needed.

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/>

## Document History

Version	Date	Description
1.0	2021-07-09	Initial version