Cyber Security Advisory #07/2021

Denial of Service vulnerability in B&R Industrial Automation PROFINET IO Devices

Document Version: 1.0

First published: 2021-07-05
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-2021-20986 Denial of Service vulnerability in B&R Industrial Automation PROFINET IO Devices
Improper buffer restrictions in in PROFINET I/O of B&R Industrial Automation products X20IF10E3-1 revisions prior to 1.8, 20cIF10E3-1 revisions prior to 1.8 and 5ACPCI.XPNS-00 revision 1.5.1.0 and prior revisions may allow unauthenticated and network based attackers to potentially enable a denial of service.

Affected Products

Affected B&R products are listed in table 1.

Material Number	Affected hardware revision	Patched hardware revision	Patch Availability
X20IF10E3-1	<1.8	1.8.0.0	June 2021
X20cIF10E3-1	<1.8	1.8.0.0	June 2021
5ACPCI.XPNS-00	<=1.5.1	1.8.0.0	June 2021

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

The time period in Table 1 denoted as planned is preliminary and may be subject to change. Registered customers may approach their local B&R service organization in case of questions.

Vulnerability ID

CVE-2021-20986 Denial of Service vulnerability in B&R Industrial Automation PROFINET IO Devices

Vulnerability Severity

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

CVE-2021-20986 Denial of Service vulnerability in B&R Industrial Automation PROFINET IO Devices
CVSS v3 Base Score: 7,5 (High)
CVSS v3 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Corrective Actions or Resolution

The described vulnerabilities will be fixed in the product versions as listed in Table 1.

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

Vulnerability Details

CVE-2021-20986 Denial of Service vulnerability in B&R Industrial Automation PROFINET IO Devices

Description

B&R products X20IF10E3-1, X20cIF10E3-1 and 5ACPCI.XPNS-00 are affected by a vulnerability by a Hilscher PROFINET IO Device.
When handling Read Implicit Request services, depending on the content of the request, the Hilscher PROFINET IO Device V3 protocol stack does not properly limit available resources. This could lead to shortage of resources which in the end could lead to unexpected loss of cyclic communication or interruption of acyclic communication.

Impact

An attacker could leverage this vulnerability so the device may no longer perform acyclic requests, drop all established cyclic connections and disappear completely from network

Workarounds and Mitigations

B&R has not identified any workarounds or mitigating factors.
In general, B&R recommends implementing the B&R Cyber Security Guideline

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/

References

[1] Hilscher Cyber Security

https://kb.hilscher.com/display/ISMS/2020-12-03+Denial+of+Service+vulnerability+in+PROFINET+IO+Device

Document History

Version	Date	Description
1.0	2021-07-05	Initial version