PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #06/2021

Stack crash in B&R Industrial Automation X20 EthernetIP Adapter

Document Version: 1.0

First published: 2021-07-05
Last updated: N/A (Initial version)

Executive Summary

CVE-2021-20987 Stack crash in B&R Industrial Automation X20 EthernetIP Adapter
Improper buffer restrictions in the EtherNet/IP component of B&R Industrial Automation X20IF10D3-1 revisions prior to 1.5 and X20cIF10D3-1 revisions prior to 1.5 may allow an unauthenticated and network based attacker to potentially enable a denial of service or to execute code.

Affected Products

Affected versions: Please refer to Table 1

Material Number	Affected hardware revision	Patched hardware revision	Patch Availability
X20IF10D3-1	<1.5.0.0	1.5.0.0	Sept 2020
X20cIF10D3-1	<1.5.0.0	1.5.0.0	Sept 2020

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

Vulnerability ID

CVE-2021-20987 Stack crash in B&R Industrial Automation X20 EthernetIP Adapter

Vulnerability Severity

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

CVE-2021-20987 Stack crash in B&R Industrial Automation X20 EthernetIP Adapter
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-2021-20987 Stack crash in B&R Industrial Automation X20 EthernetIP Adapter

Description

B&R products X20IF10E3-1 and X20cIF10E3-1 are affected by a vulnerability of Hilscher EtherNet/IP Core V2.
The EtherNet/IP Core V2 processes a CIP service request received from the network. During that process, the attached service data is copied into an internal buffer without checking the size of the data.

This can result in memory corruption which in turn could be used for remote code injection and a denial-of-service attack.

Impact

An attacker could leverage this vulnerability with specially crafted packets which may cause denial of service, remote code execution and code exposure

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/pages/viewpage.action?pageId=108969480

Document History

Version	Date	Description
1.0	2021-07-05	Initial version