Cyber Security Advisory #02/2021

Denial-of-Service Vulnerability handling PROFINET DCE-RPC Network Packets

Document Version: 1.0

First published: 2021-04-30
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-2019-13946 Denial-of-Service Vulnerability handling PROFINET DCE-RPC Network Packets
A resource allocation issue in multiple B&R I/O system and HMI components could allow an unauthenticated attacker, with network access to cause a denial of service (DoS) condition.

Affected Products

B&R HMI Products

Affected B&R HMI products are listed in Table 1.

Material Number	Affected hardware revision
4B1400.00-K30	<=E0
4B1400.00-K32	<=E0
4B1400.00-K59	<=D0
4B1400.00-K60	<=D0
4B1400.00-K63	<=C0
4B1400.00-K64	<=E0
4B1400.00-K65	<=D0
4B1400.00-K68	<=E0
4B1400.00-K69	<=D0
4B1400.00-K70	<=E0
4B1400.00-K73	<=D0
5AP933.156B-K12	<=A0
5AP93D.156C-K01	<=G0
5PC725.1505-K15	<=H0
5PC725.1505-K16	<=D0
5PC725.1505-K17	<=C0
5PC725.1505-K25	<=G0
5PC725.1505-K26	<=E0
5PC725.1505-K27	<=C0
5PC725.1505-K14	<=I0
5PC725.1505-K24	<=I0

Table 1: Affected B&R HMI products

B&R I/O system product

Affected B&R I/O system products are listed in Table 2.

Material Number	Affected hardware revision
X20BC00E3	<=D9
X20cBC00E3	<=D9
X67BCE321.L12	<=C9

Table 2: Affected B&R I/O system products

Vulnerability ID

CVE-2019-13946 Denial-of-Service Vulnerability handling PROFINET DCE-RPC Network Packets

Vulnerability Severity

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

CVE-2019-13946 Denial-of-Service Vulnerability handling PROFINET DCE-RPC Network Packets

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vulnerability Details

CVE-2019-13946 Denial-of-Service Vulnerability handling PROFINET DCE-RPC Network Packets

Description

Affected B&R products do not properly limit internal resource allocation when handling PROFINET DCE-RPC network packets. This security issue originates from the implemented PROFINET-IO network stack[1].

Impact

Adversaries may trigger Denial-of-Service (DoS) on the affected B&R products, thus compromising the availability of the device.

Fix

B&R does not provide patches for this vulnerability.
B&R recommends addressing the cyber security risk originating from this security issue by implementing the recommendations in section Workarounds and Mitigations.

Workarounds and Mitigations

B&R recommends the following specific workarounds and mitigations:
DCE-RPC network communication should be restricted to legitimate network partners, using e.g. a sufficient Firewall setup and robust network segmentation.
It is recommended to block incoming DCE-RPC network packets (port 34964/udp) from untrusted networks.

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] Denial-of-Service Vulnerability in PROFINET Devices via DCE-RPC Packets

`https://cert-portal.siemens.com/productcert/pdf/ssa-780073.pdf`

Document History

Version	Date	Description
1.0	2021-04-30	Initial version