PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #13/2021

Number:Jack in B&R Products

Document Version: 1.0

First published: 2021-11-30
Last updated: N/A (Initial version)

Notice

Executive Summary

CVE-2020-27634 ISN generator is initialized with a constant value and has constant increments
Forescout Research Labs disclosed Number:Jack, a set of vulnerabilities in multiple TCP/IP stacks in which ISNs (Initial Sequence Numbers within TCP connections) are improperly generated, leaving TCP connections of a device open to attacks. B&R uses one of the affected IP stacks in products of the groups

- Vision cameras
- Safe Logic
- Bus Controller
- Motion components

Affected Products

Affected versions: Please refer to Table 1 and Table 2

Software product	Affected Versions	Patched Version	Patch Availability
ACP10	<5.15.0	5.15.0	Available
Acp10Arnc0	<5.15.0	5.15.0	Available

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

Material Number	Affected hardware /firmware version	Patched hardware /firmware version	Patch Availability
8B0C*	HW <=1.0.0.4	TBA	Release pending
8CVE*	HW <=1.0.0.3	-	No fix planned
8I66xxxxxxx.0P-xxx	HW <2.4.0.0	HW 2.4.0.0	Available
8I76xxxxxxx.0P-xxx	HW <2.4.0.0	HW 2.4.0.0	Available
8I86xxxxxxx.0P-1xx	HW <2.4.0.0	HW 2.4.0.0	Available
8I86xxxxxxx.0P-2xx	HW <2.4.0.0	HW 2.4.0.0	Available
PLCBC0083	HW <2.14.1.0	HW 2.14.1.0	Available
SE0BC0088	FW <=3.11	TBA	Release pending
SE0BC00H3	FW <=1.50	TBA	Release pending
SE0SLH000	FW <=1.50	TBA	Release pending
SE0SLH000-1	FW <=1.50	TBA	Release pending
SE0SLH001-1	FW <=1.50	TBA	Release pending
VSS*	FW <110	FW110 (HW 1.4.0.x)	Available
X20(c)BC0083	HW <2.14.0.0	HW 2.14.0.0	Available
X20(c)BC0087	FW <=1.50	TBA	Release pending
X20(c)BC0088	FW <=3.11	TBA	Release pending
X20(c)BC1083	HW <2.14.0.0	HW 2.14.0.0	Available
X20(c)BC8083	HW <2.14.0.0	HW 2.14.0.0	Available
X20(c)BC8084	HW <2.14.0.0	HW 2.14.0.0	Available
X20(c)HB8815	HW <1.7.0.0	HW 1.7.0.0	Available
X20BC0087-10	FW <=1.50	TBA	Release pending
X20BC0087-C01	FW <=1.50	TBA	Release pending
X20BC00E3	FW <=4.04	FW 4.05	Release pending
X20BC00G3	FW <=1.28	TBA	Release pending
X20BC00H3	FW <=2.79	TBA	Release pending

X20BC00H3-C01	FW <=2.79	TBA	Release pending
X20cBC00E3	FW <=4.04	FW 4.05	Release pending
X20HB28G0	FW <=1.28	-	Maintenance discontinued
X20HB88G0	FW <=1.28	-	Maintenance Discontinued
X20SL81xx	HW <2.4.2.0	HW 2.4.2.0	Available
X67BC81RT.L12	HW <2.14.0.0	HW 2.14.0.0	Available
X67BC8321.L12	HW <2.14.0.0	HW 2.14.0.0	Available
X67BC8321-1	HW <2.14.0.0	HW 2.14.0.0	Available
X67BC8331	HW <2.14.0.0	HW 2.14.0.0	Available
X67BC8513.L12	HW <2.14.1.0	HW 2.14.1.0	Available
X67BC8513.L12-1	HW <2.14.0.0	HW 2.14.0.0	Available
X67BC8591.L12	HW <2.14.1.0	HW 2.14.1.0	Available
X67BCD321.L12	FW <=3.11	TBA	Release pending
X67BCD321.L12-1	FW <=3.11	TBA	Release pending
X67BCE321.L12	FW <=4.04	FW 4.05	Release pending
X67BCG321.L12	FW <=1.50	TBA	Release pending
X67BCJ321	FW <=1.50	TBA	Release pending
X67BCJ321.L12	FW <=1.50	TBA	Release pending

Table 2: Overview on affected hardware, patched versions and release dates

Vulnerability ID

CVE-2020-27634 ISN generator is initialized with a constant value and has constant increments

Vulnerability Severity

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

CVE-2020-27634 ISN generator is initialized with a constant value and has constant increments
CVSS v3.1 Score: 5,7 (Medium)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C

Corrective Actions or Resolution

The described vulnerabilities have been fixed in the product versions as listed in Table 1.
Information about the availability of patches will be updated periodically.

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

Vulnerability Details

CVE-2020-27634 ISN generator is initialized with a constant value and has constant increments

Description

The Initial Sequence Number (ISN) of B&R vision cameras, safe logics, bus controller and motion components is initialized with a constant value and has constant increments. This results in the ISN being able to be calculated.

Impact

An unauthorized and network based attacker could leverage this vulnerability to potentially hijack an ongoing connection or spoof a new one

Workarounds and Mitigations

B&R has not identified any workarounds or mitigating factors.
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	2021-11-30	Initial version