PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #04/2021

Amnesia:33 – Impact on B&R Products

Document Version: 1.1

First published: 2021-05-27
Last updated: 2021-09-10

Executive Summary

B&R is aware of a series of vulnerabilities disclosed by Forescout, known as Amnesia:33 (hereafter called "Amnesia"). Amnesia comprises 33 vulnerabilities in 4 open source TCP/IP stacks designed for embedded systems.

One B&R POWERLINK stack includes a proprietary TCP/IP stack which is related to a TCP/IP stack affected by Amnesia. B&R has discovered that this proprietary TCP/IP stack is affected by two Amnesia vulnerabilities. Since the affected TCP/IP stack is a part of it, the POWERLINK stack is affected too.

The affected POWERLINK stack is used by a range of B&R field-level products. This means that the following product categories are affected by the two Amnesia vulnerabilities discussed in this document:

- B&R Ethernet-based Bus Controllers and related products
- B&R Ethernet-based Customized HMI devices (e.g. Keyboards)
- B&R Motion Control products
- B&R Track Technology products

Vulnerable B&R field-level products reside in a POWERLINK network. At the network topology level, the POWERLINK network is separated from the control network – illustrated by the example of a typical B&R X20 PLC configuration:

- The control network is connected to Ethernet interface IF2
- The POWERLINK network is connected to Ethernet interface IF3

Despite this separation, certain B&R products route IP packets between POWERLINK networks and other networks like the control network. Depending on type and configuration of deployed B&R products and depending on the network configuration, vulnerable B&R products inside POWERLINK networks may be reachable from other networks.

Affected Products

The following product categories are affected by the two Amnesia vulnerabilities discussed in this document:

- B&R Ethernet-based Bus Controllers and related products
- B&R Ethernet-based Customized HMI devices (e.g. Keyboards)
- B&R Motion Control products
- B&R Track Technology products

A list of affected products is located in *Appendix A: List of affected products*.

Vulnerability ID

CVE-2020-13987 Out-of-bounds read when calculating the checksums for IP packets
CVE-2020-17438 Out-of-bounds write when reassembling fragmented IP packets

Vulnerability Severity

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

CVE-2020-13987 Out-of-bounds read when calculating the checksums for IP packets
CVSS v3.1 Base Score: 8.2 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

CVE-2020-17438 Out-of-bounds write when reassembling fragmented IP packets
CVSS v3.1 Base Score: 7.0 (High)
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H

Corrective Actions or Resolution

B&R has evaluated all affected products regarding options to create firmware fixes. B&R has already released fixed firmware for a portion of the affected products. For other groups of affected products, B&R is preparing the release of fixed firmware.

The tables in *Appendix A: List of affected products* include the column “Firmware (FW) Fix Information”, which shows the current status of fix availability for every affected product.

In case of questions regarding the affected products, please approach your B&R service contact.

Workarounds and Mitigations

Since certain B&R products route IP packets between POWERLINK networks and other networks like the control network, affected B&R products inside POWERLINK networks may be reachable from other networks. Effective network reachability of affected B&R products in a customer environment depends on type and configuration of deployed B&R products and depends on the configuration of the customer network.

Customers running affected B&R products are advised to evaluate if these products are reachable from non-POWERLINK networks. If this is the case, customers are advised to evaluate options to protect affected B&R products. Protection options are presented in the B&R guideline “General recommendations for safeguarding control systems” referenced in section *Supporting information and guidelines*.

Vulnerability Details

CVE-2020-13987 Out-of-bounds read when calculating the checksums for IP packets

Description

The TCP/IP stack code fails to check relevant packet header fields against the data available in the packets. As a result, an out-of-bounds memory read may be performed during the checksum computation.

Impact

An adversary may send crafted packets to affected products, potentially resulting in a denial of service condition.

Fix

The relevant B&R TCP/IP stack code has been corrected.

CVE-2020-17438 Out-of-bounds write when reassembling fragmented IP packets

Description

The TCP/IP stack code fails to perform certain validation checks when processing fragmented packets, potentially leading to an out-of-bounds memory write operation.

Impact

An adversary may send crafted packets to affected products, potentially resulting in a denial of service condition.

Fix

The relevant B&R TCP/IP stack code has been corrected.

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	2021-05-27	Initial version
1.1	2021-09-10	List of upgrade versions updated

Appendix A: List of affected products

The following pages show a list of products which are affected by the two Amnesia vulnerabilities discussed in this document. B&R has compiled this list to the best of our knowledge and might amend this list with additional affected products.

Description of Firmware (FW) Fix Information

The entries in the column “Firmware (FW) Fix Information” found in the tables below have the following meaning:

Column entry	Description
FW maintenance discontinued	The product firmware is no longer maintained. B&R will not provide fixed firmware for this product.
No FW fix planned	B&R currently has no plans to provide fixed firmware for this product.
FW release pending	B&R will release fixed firmware for this product. The release date has not been defined yet.
Fix available: HW upgrade a.b.c.d / FW vx.y.z	B&R has released fixed firmware for this product. The fix is included in the mentioned HW upgrade version / firmware version and can be obtained from the B&R download page.
FW provided to customer	The fixed firmware for a customized product has been provided to the customer.

B&R Ethernet-based Bus Controllers and related products

Material Number	Firmware (FW) Fix Information
0AC182.1	FW maintenance discontinued
0AC182.1-DAN	FW maintenance discontinued
8I76xxxxxxx.0P-xxx	Fix available: HW upgrade 2.4.0.0
8I86xxxxxxx.0P-2xx	Fix available: HW upgrade 2.4.0.0
8I86xxxxxxx.0P-1xx	Fix available: HW upgrade 2.4.0.0
8I66xxxxxxx.0P-xxx	Fix available: HW upgrade 2.4.0.0
8I0IF248.300-1	FW maintenance discontinued
8SEI0IF248.300-1	FW release pending
EMF2191IB	FW maintenance discontinued
LD0BC1083	FW release pending
PLCBC0083	FW release pending
SE0BC0088	FW release pending
SE0BC00H3	FW release pending
SE0SLH000	FW release pending
SE0SLH000-1	FW provided to customer
SE0SLH001	FW release pending
SE0SLH001-1	FW provided to customer
VSBLCP.13PMA-1	FW release pending
VSBLCP.15PMA-1	FW release pending
VSBLCP.16PMA-1	FW release pending
VSBLCP.18PMA-1	FW release pending
VSBLCP.1APMA-1	FW release pending
VSBLCP.1DPMA-1	FW release pending
VSBLCP.1FPMA-1	FW release pending
VSBLCP.1HPMA-1	FW release pending
VSBLCP.1QPMA-1	FW release pending
VSBLCP.1RPMA-1	FW release pending
VSBLCP.1SPMA-1	FW release pending
VSBLCP.2HPMA-1	FW release pending
VSLBMA-1	FW release pending
VSLBSTD-1	FW release pending
VSLF111Q2.00AP-E01	FW maintenance discontinued

VSS112001.041P-E01	FW maintenance discontinued
VSS112001.041P-E02	FW maintenance discontinued
VSS112001.071P-E02	FW maintenance discontinued
VSS112002.031P-E01	FW maintenance discontinued
VSS112002.051P-E02	FW maintenance discontinued
VSS112821.051P-E01	FW maintenance discontinued
VSS112821.051P-E02	FW maintenance discontinued
VSS112821.052P-E02	FW maintenance discontinued
VSS112831.071P-E02	FW maintenance discontinued
VSS112A31.061P-E02	FW maintenance discontinued
VSS112F11.021P-E02	FW maintenance discontinued
VSS112F21.042P-E02	FW maintenance discontinued
VSS112F21.061P-E02	FW maintenance discontinued
VSS112F31.071P-E02	FW maintenance discontinued
VSS112Q11.022P-E02	FW maintenance discontinued
VSS112Q11.031P-E02	FW maintenance discontinued
VSS112Q11.041P-E01	FW maintenance discontinued
VSS112Q12.021P-E02	FW maintenance discontinued
VSS112Q12.032P-E02	FW maintenance discontinued
VSS112Q21.022P-E02	FW maintenance discontinued
VSS112Q21.042P-E02	FW maintenance discontinued
VSS112Q21.051P-E02	FW maintenance discontinued
VSS112Q21.061P-E01	FW maintenance discontinued
VSS112Q21.061P-E02	FW maintenance discontinued
VSS112Q21.062P-E02	FW maintenance discontinued
VSS112Q21.081P-E01	FW maintenance discontinued
VSS112Q21.121P-E01	FW maintenance discontinued
VSS112Q21.M51P-E01	FW maintenance discontinued
VSS112Q22.031P-E02	FW maintenance discontinued
VSS112Q22.041P-E02	FW maintenance discontinued
VSS112Q22.081P-E01	FW maintenance discontinued
VSS112Q22.121P-E01	FW maintenance discontinued
VSS112Q22.M51P-E02	FW maintenance discontinued
VSS112Q24.061P-E01	FW maintenance discontinued
VSS112Q31.071P-E02	FW maintenance discontinued
VSS112R11.031P-E02	FW maintenance discontinued
VSS112R11.041P-E02	FW maintenance discontinued
VSS112R21.041P-E01	FW maintenance discontinued
VSS112R21.061P-E01	FW maintenance discontinued
VSS112R21.062P-E02	FW maintenance discontinued
VSS112R22.041P-E02	FW maintenance discontinued

VSS112R22.051P-E02	FW maintenance discontinued
VSS112R22.061P-E02	FW maintenance discontinued
VSS112R31.041P-E01	FW maintenance discontinued
VSS112S21.061P-E01	FW maintenance discontinued
VSSCP112.P-1	Fix available: HW upgrade 1.3.0.x
VSSCP112.P-12	Fix available: HW upgrade 1.3.0.x
VSSCP112.P-2	Fix available: HW upgrade 1.3.0.x
VSSCP112.P-22	Fix available: HW upgrade 1.3.0.x
VSSCP122.P-1	Fix available: HW upgrade 1.3.0.x
VSSCP122.P-12	Fix available: HW upgrade 1.3.0.x
VSSCP122.P-2	Fix available: HW upgrade 1.3.0.x
VSSCP122.P-22	Fix available: HW upgrade 1.3.0.x
X20BC0083	FW release pending
X20BC0087	FW release pending
X20BC0087-10	FW release pending
X20BC0087-C01	FW release pending
X20BC0088	FW release pending
X20BC00E3	FW release pending
X20BC00H3	FW release pending
X20BC00H3-C01	FW release pending
X20BC1083	FW release pending
X20BC8083	FW release pending
X20BC8084	FW release pending
X20CBC0083	FW release pending
X20CBC0087	FW release pending
X20CBC0088	FW release pending
X20CBC00E3	FW release pending
X20CBC1083	FW release pending
X20CBC8083	FW release pending
X20CBC8084	FW release pending
X20CHB8815	Fix available: HW upgrade 1.7.0.0
X20CSL8000	FW maintenance discontinued
X20CSL8001	FW maintenance discontinued
X20CSL8100	Fix available: HW upgrade 1.10.10.2

X20CSL8101	Fix available: HW upgrade 1.10.10.2
X20ET8819	Fix available: FW upgrade V1.11
X20HB8815	Fix available: HW upgrade 1.7.0.0
X20SL8000	FW maintenance discontinued
X20SL8001	FW maintenance discontinued
X20SL8010	FW maintenance discontinued
X20SL8011	FW maintenance discontinued
X20SL8100	Fix available: HW upgrade 1.10.10.2 HW upgrade 2.4.1.0
X20SL8101	Fix available: HW upgrade 1.10.10.2 HW upgrade 2.4.1.0
X20SL8110	Fix available: HW upgrade 1.10.10.2 HW upgrade 2.4.1.0
X67BC81RT.L12	FW release pending
X67BC8321.L12	FW release pending
X67BC8321-1	FW release pending
X67BC8331	FW release pending
X67BC8513.L12	FW release pending
X67BC8513.L12-1	FW release pending
X67BC8591.L12	FW release pending
X67BC8780.L12	FW release pending
X67BCD321.L12	FW release pending
X67BCD321.L12-1	FW release pending
X67BCE321.L12	FW release pending
X67BCH321.L12	FW release pending
X67BCJ321	FW release pending
X67BCJ321.L12	FW release pending

B&R Ethernet-based Customized HMI devices (e.g. Keyboards)

Material Number	Firmware (FW) Fix Information
4B1400.00-K21	No FW fix planned
4B1400.00-K33	No FW fix planned
4B1400.00-K34	No FW fix planned
4B1400.00-K35	No FW fix planned
4B1400.00-K36	No FW fix planned
4B1400.00-K37	No FW fix planned
4B1400.00-K38	No FW fix planned
4B1400.00-K39	No FW fix planned
4B1400.00-K40	No FW fix planned
4B1400.00-K42	No FW fix planned
4B1400.00-K43	No FW fix planned
4B1400.00-K44	No FW fix planned
4B1400.00-K45	No FW fix planned
4B1400.00-K47	No FW fix planned
4B1400.00-K48	No FW fix planned
4B1400.00-K50	No FW fix planned
4B1400.00-K51	No FW fix planned
4B1400.00-K53	No FW fix planned
4B1400.00-K56	No FW fix planned
4B1400.00-K57	No FW fix planned
4B1400.00-K58	No FW fix planned
4B1400.00-K62	No FW fix planned
4B1400.00-K67	No FW fix planned
4B1400.00-K71	No FW fix planned
4B1400.00-K72	No FW fix planned
4SIM.10-01	No FW fix planned
5ACCKP01.215C-C04	No FW fix planned
5ACCKPPL.215C-C01	No FW fix planned
5ACCKPS0.215C-C01	No FW fix planned
5AP1120.1214-C03	No FW fix planned
5AP5335.215C-C01	No FW fix planned
5AP920.1505-K05	No FW fix planned
5AP920.1505-K10	No FW fix planned
5AP920.1505-K59	No FW fix planned
5AP920.1906-K23	No FW fix planned
5AP923.1505-K04	No FW fix planned
5AP923.156B-K02	No FW fix planned
5AP923.215C-K01	No FW fix planned

5AP92D.1214-K01	No FW fix planned
5AP92D.1214-K02	No FW fix planned
5AP92D.215I-K02	No FW fix planned
5AP933.156B-K01	No FW fix planned
5AP933.156B-K02	No FW fix planned
5AP933.215I-K01	No FW fix planned
5AP93D.185B-K01	No FW fix planned
5AP93D.215C-K01	No FW fix planned
5AP93D.215C-K07	No FW fix planned
5AP950.1706-K03	No FW fix planned
5AP950.1706-K04	No FW fix planned
5AP980.1505-K15	No FW fix planned
5AP980.1505-K17	No FW fix planned
5AP980.1505-K29	No FW fix planned
5AP980.1906-K07	No FW fix planned
5AP980.1906-K08	No FW fix planned
5E9000.35	No FW fix planned
5E9000.44	No FW fix planned
5E9000.46	No FW fix planned
5E9000.50	No FW fix planned
5E9000.53	No FW fix planned
5PC720.1505-K18	No FW fix planned

B&R Motion Control products

Material Number	Firmware (FW) Fix Information
8AC114*	Fix available: FW v5.13.2
8B0P*	Fix available: FW v5.13.2
8BVI*	Fix available: FW v5.13.2
8BVP*	Fix available: FW v5.13.2
8CVE*	No FW fix planned
8CVI*	Fix available: FW v5.13.2
8DI*	Fix available: FW v5.13.2
8EI*	Fix available: FW v5.13.2
80VD*	Fix available: FW v5.13.2

B&R Track Technology products

Material Number	Firmware (FW) Fix Information
8F1I01.AA66.0000-1	Fix available: FW v5.13.2
8F1I01.AA66.0100-1	Fix available: FW v5.13.2
8F1I01.AB2B.0000-1	Fix available: FW v5.13.2
8F1I01.AB2B.0100-1	Fix available: FW v5.13.2
8F1I01.BA2B.0000-1	Fix available: FW v5.13.2
8F1I01.BA2B.0100-1	Fix available: FW v5.13.2
8F1I01.BB4B.0000-1	Fix available: FW v5.13.2
8F1I01.BB4B.0100-1	Fix available: FW v5.13.2