PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #01/2019

B&R Products affected by VxWorks IPnet Vulnerabilities (Urgent/11)

Document Version: 1.1

First published: 2019-08-07
Last updated: 2021-02-22

Notice

1. Executive summary

IoT security company Armis reported a total of 11 vulnerabilities called “Urgent/11” to Wind River. These vulnerabilities affect VxWorks, a real-time operating system (RTOS) manufactured by Wind River.
Detailed information about the vulnerabilities are available on Wind River’s website [1] [2] and on Armis’ website [3].

B&R Automation Runtime software is based on VxWorks and these vulnerabilities affect a range of Automation Runtime versions listed in section “Affected Products”.
To address these vulnerabilities, B&R has integrated patches into affected Automation Runtime versions. Fixed Automation Runtime versions are presented in section “Corrective Actions or Resolution”.

The following table lists the individual Urgent/11 vulnerabilities:

CVE ID	Title	CVSSv3 Score	CVSSv3 Severity
CVE-2019-12256	Stack overflow in the parsing of IPv4 packets’ IP options	9.8	Critical
CVE-2019-12257	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc	8.8	High
CVE-2019-12255	TCP Urgent Pointer = 0 leads to integer underflow	9.8	Critical
CVE-2019-12260	TCP Urgent Pointer state confusion caused by malformed TCP AO option	9.8	Critical
CVE-2019-12261	TCP Urgent Pointer state confusion during connect() to a remote host	8.8	High
CVE-2019-12263	TCP Urgent Pointer state confusion due to race condition	8.1	High
CVE-2019-12258	DoS of TCP connection via malformed TCP options	7.5	High
CVE-2019-12259	DoS via NULL dereference in IGMP parsing	6.3	Medium
CVE-2019-12262	Handling of unsolicited Reverse ARP replies (Logical Flaw)	7.1	High
CVE-2019-12264	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	7.1	High
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report	5.4	Medium

The maximum value of a CVSSv3 score is 10.0, indicating the most severe kind of a vulnerability.

2. Affected Products

The Urgent/11 vulnerabilities affect a range of Automation Runtime versions used in various B&R products.

The matrix below maps the Urgent/11 vulnerabilities to Automation runtime versions and shows which Automation Runtime version is affected by which vulnerability:

CVE ID	Affected Module	CVSSv3 Score	Title/Description	AR 2.x	AR 3.x	AR 4.00 to 4.09	AR 4.10 to 4.63
CVE-2019-12256	TCP/IP-stack	9.8	Stack overflow in the parsing of IPv4 packets IP options	no	no	no	yes
CVE-2019-12257	DHCP Client	8.8	Heap overflow in DHCP Offer/ACK parsing inside idphcpc	no	no	yes	no
CVE-2019-12255	TCP/IP-stack	9.8	TCP Urgent Pointer = 0 leads to integer underflow	no	no	yes	no
CVE-2019-12260	TCP/IP-stack	9.8	TCP Urgent Pointer state confusion caused by malformed TCP AO option	no	no	no	no
CVE-2019-12261	TCP/IP-stack	8.8	TCP Urgent Pointer state confusion during connect() to a remote host	no	no	yes	yes
CVE-2019-12263	TCP/IP-stack	8.1	TCP Urgent Pointer state confusion due to race condition	no	no	yes	yes
CVE-2019-12258	TCP/IP-stack	7.5	DoS of TCP connection via malformed TCP options	no	no	yes	yes
CVE-2019-12259	TCP/IP-stack	6.3	DoS via NULL dereference in IGMP parsing	no	no	yes	yes
CVE-2019-12262	TCP/IP-stack	7.1	Handling of unsolicited Reverse ARP replies (Logical Flaw)	no	no	yes	yes
CVE-2019-12264	DHCP Client	7.1	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	no	no	yes	yes
CVE-2019-12265	TCP/IP-stack	5.4	IGMP Information leak via IGMPv3 specific membership report	no	no	yes	yes

Yes: AR version is affected by the vulnerability / No: AR version is immune to the vulnerability

Figure 1: Mapping of Urgent/11 vulnerabilities to Automation Runtime (“AR”) versions

3. Corrective Actions or Resolution

The Urgent/11 vulnerabilities have been fixed in the following Automation Runtime versions:

Fixed AR versions
T4.10
M4.26
M4.34
E4.45
C4.53
C4.63
C4.72

Automation Runtime versions 4.00 to 4.09 will not be fixed. Customers using these versions are advised to approach their B&R technical contact regarding an upgrade to a newer Automation Runtime version.

4. Safeguarding Measures/Mitigations

Measures to minimize risks arising from exploits leveraging Urgent/11 vulnerabilities are presented in the "General recommendations for safeguarding control systems" on the B&R Cyber Security webpage.

5. Further details and information sources

[1]
Wind River Urgent/11 Security Vulnerability Response Information:
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

[2]
Wind River Urgent/11 Security Advisory:
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/security-advisory-ipnet/

[3]
Armis Urgent/11 information page:
https://armis.com/urgent11/