PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory 01/2019

Wind River VxWorks IPnet Vulnerabilities (Urgent/11)

Impact on B&R products

Document Version: 1.0
Release Date: 7th of August, 2019

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

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.

1. Overview

IoT security company Armis reported a total of 11 vulnerabilities called “Urgent/11” to WindRiver. These vulnerabilities affect VxWorks, a real-time operating system (RTOS) running on various devices like industrial control systems. Wind River published these vulnerabilities in their security advisory. The vulnerabilities affect VxWorks versions 6.5 up to the current versions 6.9.x and 7.x.
Information on the vulnerabilities and their possible impacts are given in section 4.
Detailed information about the vulnerabilities are available on Wind River’s website [1] [2] and on Armis’ website [3] [4].

B&R Automation Runtime software is based on VxWorks and these vulnerabilities affect a range of Automation Runtime versions.
To address these vulnerabilities, patches will be integrated into Automation Runtime and will be provided as maintenance releases for Automation Runtime versions affected by Urgent/11. In the meantime customers are encouraged to take safeguarding measures to minimize risks arising from exploitation of Urgent/11 vulnerabilities as outlined below.

The Urgent/11 vulnerability CVE numbers and titles are listed in the table below:

CVE	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 highest value a CVSSv3 score can have 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	Affected Module	CVSSv3 Score	Title/Description	AR 2.x	AR 3.x	AR 4.00 to 4.05	AR 4.06 to 4.09	AR 4.10 to 4.63
			Underlying VxWorks version	5.4	5.4	6.8	6.9.2.2	6.9.4.1
CVE-2019-12256	TCP/IP-stack	9.8	Stack overflow in the parsing of IPv4 packets IP options	no	no	no	no	yes
CVE-2019-12257	DHCP Client	8.8	Heap overflow in DHCP Offer/ACK parsing inside idphcpc	no	no	yes	yes	no
CVE-2019-12255	TCP/IP-stack	9.8	TCP Urgent Pointer = 0 leads to integer underflow	no	no	yes	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	yes
CVE-2019-12261	TCP/IP-stack	8.8	TCP Urgent Pointer state confusion during connect() to a remote host	no	no	yes	yes	yes
CVE-2019-12263	TCP/IP-stack	8.1	TCP Urgent Pointer state confusion due to race condition	no	no	yes	yes	yes
CVE-2019-12258	TCP/IP-stack	7.5	DoS of TCP connection via malformed TCP options	no	no	yes	yes	yes
CVE-2019-12259	TCP/IP-stack	6.3	DoS via NULL dereference in IGMP parsing	no	no	yes	yes	yes
CVE-2019-12262	TCP/IP-stack	7.1	Handling of unsolicited Reverse ARP replies (Logical Flaw)	no	no	yes	yes	yes
CVE-2019-12264	DHCP Client	7.1	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	no	no	yes	yes	yes
CVE-2019-12265	TCP/IP-stack	5.4	IGMP Information leak via IGMPv3 specific membership report	no	no	yes	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. Safeguarding Measures/Mitigations

Customers are to take the following measures to minimize risks arising from exploits leveraging Urgent/11 vulnerabilities:

a. Place industrial control systems (ICS) in a dedicated network containing ICS components only
b. Use firewalls to isolate ICS networks from all other (e.g. business) networks
c. Create firewall rules to filter network traffic targeting Urgent/11 vulnerabilities (“exploit traffic”)
d. Optional: Use Intrusion Detection Systems (IDS) to monitor your networks for exploit traffic
e. Optional: Use Intrusion Preventions Systems (IPS) to protect ICS from exploit traffic

Caution
Please use caution when implementing safeguarding measures. It is your responsibility to make sure such measures do not have side effects interfering with normal ICS operations.

General ICS Security Guidelines

- Locate ICS networks and devices behind firewalls and isolate them from any other networks like business networks.
- Make sure ICS networks/devices are not accessible from the Internet.
- Block any inbound Internet traffic destined for the ICS network/devices. Place remote access devices used for remote ICS access outside the ICS network.
- Limit outbound Internet traffic originating from ICS devices/networks as much as possible.
  If ICS devices must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which ICS devices definitely need to use for normal ICS operations.
  If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of ICS networks/devices to internal systems. Tailor firewall rules allowing traffic from internal systems to ICS networks/devices to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal ICS operations.
- If supported by your firewall and thoroughly tested in advance, apply additional filters to allowed traffic which provide protection for ICS networks/systems. Such filters are provided by advanced firewall features like IPS (Intrusion Prevention), Application Control and Anti-Virus.
- In case you use an IPS solution, consider using IPS rules protecting against ICS exploits.
- Use trusted software, software patches, Anti-Malware programs and interact only with trusted web sites and trusted email attachments.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please note that VPN solutions may have vulnerabilities and should be updated to the most current version available.

4. Vulnerability details

Vulnerability CVE-2019-12255
Title: TCP Urgent Pointer = 0 leads to integer underflow
Affected AR versions: 4.00 to 4.09
CVSS v3.0 Base Score: 9.8 / Severity: Critical

An attacker could send specially crafted TCP packets with a manipulated TCP Urgent Pointer to a vulnerable device, resulting in a Denial-of-Service (DoS) condition to the application or the execution of arbitrary code on the device.
Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12256
Title: Stack overflow in the parsing of IPv4 packets' IP options
Affected AR versions: 4.10 to 4.63
CVSS v3.0 Base Score: 9.8 / Severity: Critical

By sending IPv4 packets with specially crafted IP options to a vulnerable device, an attacker could crash the network processing task on the device and potentially execute arbitrary code on the device. Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12257
Title: Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc
Affected AR versions: 4.00 to 4.09
CVSS v3.0 Base Score: 8.8 / Severity: High

By sending specially crafted DHCP packets to a vulnerable device, an attacker could exploit this vulnerability to overwrite the heap, which may result in a crash later on when a task requests memory from the heap. Furthermore, the attacker can potentially execute arbitrary code on the device.
Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12258
Title: Denial of Service (DoS) of TCP connection via malformed TCP options
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 7.5 / Severity: High

By sending TCP packets with specially crafted TCP options to a vulnerable device, an attacker could cause an existing TCP session to be reset. The most likely outcome is a crash of the application, potentially triggering a Denial-of-Service (DoS) condition.
Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12259
Title: DoS via NULL dereference in IGMP parsing
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 6.3 / Severity: Medium

By sending specially crafted IGMP packets to a vulnerable device, an attacker could crash the network processing task on the device, potentially triggering a Denial-of-Service (DoS) condition.
Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12260
Title: TCP Urgent Pointer state confusion caused by malformed TCP AO option
Affected AR versions: 4.10 to 4.63
CVSS v3.0 Base Score: 9.8 / Severity: Critical

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a vulnerable device, an attacker could crash the application on the device, potentially triggering a Denial-of-Service (DoS) condition. Furthermore, the attacker can potentially execute arbitrary code on the device.
Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12261
Title: TCP Urgent Pointer state confusion during connect() to a remote host
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 8.8 / Severity: High

While connecting to a remote host, specially crafted TCP packets with a manipulated TCP Urgent Pointer received by a vulnerable device could crash the application on the device, potentially triggering a Denial-of-Service (DoS) condition. Furthermore, the attacker can potentially execute arbitrary code on the device.
Conducting this attack requires an attacker to have a vulnerable device connect to a malicious system or to hijack and manipulate the TCP connection initiated by the vulnerable device.

Vulnerability CVE-2019-12262
Title: Handling of unsolicited Reverse Address Resolution Protocol (ARP) replies
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 7.1 / Severity: High

By sending unsolicited reverse ARP packets to a vulnerable device, an attacker can assign IPv4 addresses to this device, potentially causing network connectivity issues if the assigned IP addresses collide with those of other machines.
Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12263
Title: TCP Urgent Pointer state confusion due to race condition
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 8.1 / Severity: High

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a vulnerable device, an attacker could crash the application on the device, potentially triggering a Denial-of-Service (DoS) condition. Furthermore, the attacker can potentially execute arbitrary code on the device.
Network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12264
Title: Logical flaw in IPv4 assignment by the ipdhcpc DHCP client
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 7.1 / Severity: High

An attacker could send specially crafted DHCP packets to a vulnerable device, which may result in the device incorrectly assigning a multicast IP address chosen by the attacker. This way the attacker may be able to affect availability and integrity of the device.
Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

Vulnerability CVE-2019-12265
Title: IGMP information leak via IGMPv3 specific membership report
Affected AR versions: 4.00 to 4.63
CVSS v3.0 Base Score: 5.4 / Severity: Medium

Sending specially crafted IGMPv3 packets to a vulnerable device allow an attacker to make this device transmit packets to the network that may contain information from packets that were previously sent or received by the network stack.
Network access, but no authentication and no user interaction is needed to conduct this attack.

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/

[4]
Armis Urgent/11 Technical Whitepaper:
https://go.armis.com/hubfs/White-papers/Urgent11%20Technical%20White%20Paper.pdf

Document version information

Version	Date	Description	Author/Comment
1.0	Aug 7, 2019	First edition	PW