DOCUMENT ID:	7PAA000401
REVISION:	A
DATE:	2022-01-17
SECURITY LEVEL:	PUBLIC

CYBER SECURITY ADVISORY

SECURITY - Wind River VxWorks Multiple Vulnerabilities - Impact on Melody controller PM877

CVE ID: CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-12265, CVE-2020-35198, CVE-2020-28895

Notice

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

ABB 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 ABB 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 ABB 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 ABB, 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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations (e.g. ICS-CERT).

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

- Melody Rack - Controller PM 877. All firmware versions prior to 3.40 are affected.

Vulnerability ID

CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-12265, CVE-2020-35198, CVE-2020-28895

Summary

Wind River is the provider of a real time operating system called VxWorks which is used in the embedded software of the PM 877 Controller. Wind River has announced security vulnerabilities in the VxWorks TCP/IP stack (IPnet) and management of memory block size (Bad Alloc).

The controller PM 877 is affected by 8 of the "Urgent 11" vulnerabilities in the TCP/IP stack but it is not affected by the vulnerabilities related to memory management (Bad Alloc). All the associated vulnerabilities which impacted the PM 877 have been corrected.

An attacker who successfully exploits these vulnerabilities could hijack existing TCP sessions to inject malformed packets or steal authenticated user session identifiers, resulting in corruptions of data, unauthorized disclosure of information, denial of service and data communications outage or even code execution. The vulnerabilities do not target any ABB products specifically, but potentially affect products that use the operating system.

ABB published a Cyber Security Notification "WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation Products" (document number 8VZZ001892T0001) on the 29th of July 2019 about the TCP/IP stack vulnerability from Wind River affecting the VxWorks operating system. This advisory being published supersedes such notification and extends it with additional vulnerabilities in VxWorks (Bad Alloc).

Wind River TCP/IP stack (IPnet) vulnerabilities:

CVE	Title	Impact on PM 877
CVE-2019-12256	Stack overflow in the parsing of IPv4 packets' IP options	no
CVE-2019-12257	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc	yes
CVE-2019-12255	TCP Urgent Pointer = 0 leads to integer underflow	yes
CVE-2019-12260	TCP Urgent Pointer state confusion caused by malformed TCP AO option	yes
CVE-2019-12261	TCP Urgent Pointer state confusion during connect() to a remote host	yes
CVE-2019-12263	TCP Urgent Pointer state confusion due to race condition	yes
CVE-2019-12258	DoS of TCP connection via malformed TCP options	yes
CVE-2019-12259	DoS via NULL dereference in IGMP parsing	no
CVE-2019-12262	Handling of unsolicited Reverse ARP replies (Logical Flaw)	yes
CVE-2019-12264	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	yes
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report	no

Wind River management of memory block's size (Bad Alloc) vulnerabilities:

CVE	Title	Impact on PM 877
CVE-2020-28895	Memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc().	no
CVE-2020-35198	An issue was discovered in Wind River VxWorks 7. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by calloc().	no

Recommended immediate actions

As to the Wind River TCP/IP stack (IPnet) vulnerabilities listed above, the S+ Melody Rack - Controller PM 877 with Firmware Version < 3.40 is affected. All the vulnerabilities have been corrected in the firmware version 3.40 or later.

ABB recommends that customers apply the update at the earliest convenience.

In case one of these updates are unable to be installed, end users should immediately look to implement the Mitigation and Workarounds listed below as this will restrict an attacker's ability to compromise these systems.

Vulnerability severity and details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.0 and 3.1[1].

Herein are reported the vulnerabilities affecting the S+ Melody Rack - Controller PM 877:

CVE-2019-12257 - Heap overflow in DHCP

Wind River VxWorks 6.6 through 6.9 has a Buffer Overflow in the DHCP client component. There is an IPNET security vulnerability: Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc.

CVSS v3.0 Base Score:	8.8 High
CVSS v3.0 Vector:	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12257

CVE-2019-12255 - TCP Urgent Pointer Integer Underflow

Wind River VxWorks has a Buffer Overflow in the TCP component (issue 1 of 4). This is a IPNET security vulnerability: TCP Urgent Pointer = 0 that leads to an integer underflow.

CVSS v3.0 Base Score:	9.8 Critical
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12255

CVE-2019-12260 - TCP Urgent Pointer Malformed AO option

Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 2 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion caused by a malformed TCP AO option.

CVSS v3.0 Base Score:	9.8 Critical
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12260

CVE-2019-12261 - TCP Urgent Pointer Confusion Remote Host

Wind River VxWorks 6.7 through 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 3 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion during connect() to a remote host.

CVSS v3.0 Base Score:	9.8 Critical
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12261

[1] The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2019-12263 - TCP Urgent Pointer Confusion Race Condition

Wind River VxWorks 6.9.4 and vx7 has a Buffer Overflow in the TCP component (issue 4 of 4). There is an IPNET security vulnerability: TCP Urgent Pointer state confusion due to race condition.

CVSS v3.0 Base Score:	8.1 High
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12263

CVE-2019-12258 - DoS of TCP connection

Wind River VxWorks 6.6 through vx7 has Session Fixation in the TCP component. This is a IPNET security vulnerability: DoS of TCP connection via malformed TCP options.

CVSS v3.0 Base Score:	7.5 High
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12258

CVE-2019-12262 - Handling of Reverse ARP replies

Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and 7 has Incorrect Access Control in the RARP client component. IPNET security vulnerability: Handling of unsolicited Reverse ARP replies (Logical Flaw).

CVSS v3.0 Base Score:	9.8 Critical
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12262

CVE-2019-12264 - Logical Flaw in IPv4 Assignment

Wind River VxWorks 6.6, 6.7, 6.8, 6.9.3, 6.9.4, and Vx7 has Incorrect Access Control in IPv4 assignment by the ipdhcpc DHCP client component.

CVSS v3.0 Base Score:	7.1 High
CVSS v3.0 Vector:	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2019-12264

Mitigating factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the plant network (perimeter firewall). Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case.

Improving the PM877 isolation via a “Control Network Firewall” between the HMI and control network would help to restrict the access to the device.

Many of these vulnerabilities refer to malformed control fields of the TCP segment format: where possible, the usage of a network intrusion detection system (NIDS) or a firewall having capabilities of packet inspection could be a good mitigation.

Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Refer to section "General security recommendations" for further advice on how to keep your system secure.

Workarounds

Assess the installation specific risk based on this advisory. Use the recommendations described under "Mitigating factors" and "Recommended immediate actions".

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could affect communication on the Control Network, i.e. the network connected to the ports Onet and Eth on the PM 877 controller.

What is the VxWorks and what is the TCP/IP stack?

VxWorks is the real time operating system used by Melody PM 877 controller.

It includes e.g. the TCP/IP stack which is the SW component handling the PM 877 Ethernet Network communication. IPNet is the name of the TCP/IP stack used in the affected product versions.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could disrupt ongoing communication or block new communication on the Ethernet Network. Further, he could hijack existing TCP sessions to inject malformed packets or steal authenticated user session IDs, resulting in corruptions of data, unauthorized disclosure of information, undefined behavior (DoS, crash) or code execution.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

Can functional safety be affected by an exploit of this vulnerability?

Functional safety systems are not affected by these vulnerabilities.

What does the update do?

The update removes all the associated vulnerabilities which impacted the PM 877.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed. ABB has published the Cyber Security Notification "WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation Products" (document number 8VZZ001892T0001)
at
https://new.abb.com/about/technology/cyber-security/alerts-and-notifications. This describes that Symphony Plus Melody Rack Controller was one of the products that was using VxWorks and that further analysis was ongoing.

Information about the VxWorks vulnerabilities in the Wind River TCP/IP stack (IPnet , Urgent/11) is available here: https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

- Place control systems in a dedicated control network containing control systems only.
- Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.
- 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 control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.

- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

More information on recommended practices can be found in the following documents[2]:

2VAA003428	S+ Control Melody PM 877 User manual
8VZZ001006	Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019 user manual
2PAA121027	Distributed Control Systems - McAfee® ePO with VirusScan Enterprise, Endpoint Security and Application Control
8VZZ000602	Microsoft Security Updates Validation Status for Symphony Plus
8VZZ001753	McAfee Virus Scan DAT Update Validation Status for Symphony Plus
2PAA122516	System 800xA, Symphony Plus and Freelance System Hardening - End user manual
2PAA120528	System 800xA, Symphony Plus and Freelance System Hardening: Group Policies Overview
8VZZ000368D0066	ICS Cyber Security Reference Architecture Guide

References

8VZZ001892T0001	WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation products

[2] Access to some listed documents can be subject to the ABB Care Automation Software Maintenance specific conditions and agreements.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cyber-security.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2021-01-17