AC 800PEC – CYBER SECURITY ADVISORY

SECURITY WindRiver VxWorks IPNet Vulnerabilities - Urgent/11, impact on AC 800PEC

Vulnerability ID: ABBVU-MODR-AC 800PEC Program-27574

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.

Affected Products

Affected versions are AC 800PEC embedded software releases 5.1.0.0 and later until release 5.3.0.0. From release 5.3.0.1 onwards the issue is fixed.

This means, all ABB products that use the 3rd generation until release 5.3.0.0 of the AC 800PEC controller are potentially affected.

Vulnerability ID

ABB ID: ABBVU-MODR-AC 800PEC Program-27574

Summary

Wind River is the provider of the real time operating system VxWorks 6.8.3 which is used in the embedded software of the AC 800PEC controller.

Wind River has recently become aware of security vulnerabilities in the Wind River TCP/IP stack (IPnet) which is used in the AC 800PEC. This means that all Ethernet based protocols are affected. In certain scenarios this would lead to the controller becoming inaccessible.

The vulnerabilities do not target any ABB products specifically, but potentially affect products that use the AC 800PEC controller.

Wind River provided a patch to the AC 800PEC team which has been implemented in the embedded SW release 5.3.0.1. This document gives an overview regarding the fixed vulnerabilities.

The Wind River vulnerability CVE numbers and titles are listed in the table below:

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

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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.

Recommended immediate actions

Migrate to the latest AC 800PEC SW version 5.3.0.1. If this is for any reason not possible, minimum actions are as follows:

Recommended security practices and firewall configurations can help protect the AC 800PEC controller from attacks that originate from outside the network.

- Use the AC 800PEC within a secure network
- Add a firewall in the network. Administrators can add a rule to drop/block any TCP-segment where URG-flag is set.
- Assess the installation specific risk based on this advisory

Vulnerability Details

Vulnerabilities exist in the TCP/IP stack from VxWorks included in the product versions of the AC 800PEC listed above. An attacker could exploit these vulnerabilities.

The following list contains the description of the vulnerability related to the AC 800PEC controller. The vulnerabilities are sorted by their CVSSv3 score from top to bottom. Not all of the vulnerabilities reported by Wind River are applicable for AC 800PEC:

CVE-2019-12256: Stack overflow in the parsing of IPv4 packets' IP options

An invalid option field in the IPv4 packet header can crash the VxWorks network task tNet0, which can make the PEC controller inaccessible over the network.

No AC 800PEC SW version is affected by this issue.

CVS-2019-12255: TCP Urgent Pointer = 0 leads to integer underflow

An attacker could inject a bad TCP packet, which may lead to a buffer overflow in the TCP packet receive functions. This could lead to memory corruption and could cause a crash of the application or the PEC controller.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12260: TCP Urgent Pointer state confusion caused by malformed TCP AO option

An attacker could inject a bad TCP packet, which may lead to a buffer overflow in the TCP packet receive functions.

No AC 800PEC SW version is affected by this issue.

CVE-2019-12257: Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc

This vulnerability can be exploited only if DHCP is used during the boot process (VxWorks Bootrom) but not when starting the VxWorks from the NAND flash.

No AC 800PEC SW version is affected by this issue.

CVE-2019-12261: TCP Urgent Pointer state confusion during connect() to a remote host

An attacker could inject a bad TCP packet, which may lead to a buffer overflow in the TCP packet receive functions. This could lead to memory corruption and could cause a crash of the application or the PEC controller.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12263: TCP Urgent Pointer state confusion due to race condition

An attacker could inject a bad TCP packet, which may lead to a buffer overflow in the TCP packet receive functions. This could lead to memory corruption and could cause a crash of the application or the PEC controller.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12258: DoS of TCP connection via malformed TCP options

An attacker may inject invalid TCP segments in the network traffic. This may lead to a connection break, which may cause the application to stop working properly.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12262: Handling of unsolicited Reverse ARP replies (Logical Flaw)

An attacker can assign a wrong IPv4 address to a controller. The action will not cause any direct harm more than increased usage of RAM. However, the vulnerability may indirectly cause a network connectivity issue for the system on the LAN if the assigned IP addresses collide with other machines.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12264: Logical flaw in IPv4 assignment by the ipdhcpc DHCP client

An attacker can assign a wrong IPv4 address to a controller. In combination with CVE-2019-12259 it may create a denial-of-service attack.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12259: DoS via NULL dereference in IGMP parsing

An incorrectly assigned multicast IP address may lead to a NULL pointer dereference in the VxWorks network task tNet0, which can make the PEC controller inaccessible over the network.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

CVE-2019-12265: IGMP Information leak via IGMPv3 specific membership report

In a system where multicast addresses are used, the IGMPv3 reception handler can leak IGMP information to an attacker. The leaked information is not application critical in a PEC system.

All releases from 5.1.0.0 to 5.3.0.0 are affected.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could affect communication on the Control Network, i.e. the network connected to one for the three ethernet ports on the Processor Module of the AC 800PEC controller.

What causes the vulnerability?

The vulnerability is caused by insufficient input data validation in the TCP/IP stack in VxWorks used by the AC 800PEC controller.

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

VxWorks is the real time operating system used by AC 800PEC controller. It includes e.g. the TCP/IP stack which is the SW component handling the AC 800PEC 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 this vulnerability could disrupt ongoing communication or block new communication on the Control Network.

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 recommended immediate actions 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.

What does the update do?

These corrections remove the vulnerability by applying security updates from WindRiver that modify the way that the TCP/IP stack validates messages. The controller's network security protection measures are also extended.

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

The list of vulnerabilities in VxWorks has been publicly disclosed by Wind River. ABB has published the Cyber Security Notification "Wind River VxWorks IPNet Vulnerabilities, impact on AC 800PEC" at https://new.abb.com/about/technology/cyber-security/alerts-and-notifications. This describes that AC 800PEC was one of the products that was using VxWorks and that further analysis was ongoing.

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.

Support

For additional information and support please contact your local ABB service organization. For contact information, see http://new.abb.com/contact-centers.

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

For AC 800PEC specific questions please get in contact with the AC 800PEC team (pec@ch.abb.com).