ABB DOC ID: 2PAA120481
REVISION: B
DATE: 2021-07-02

CYBER SECURITY ADVISORY

SECURITY WindRiver VxWorks IPNet Vulnerabilities, impact on AC 800M

Vulnerability ID: ABBVU-IACT- 800xACON-OL-5114-001

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

AC 800M and AC 800M HI with versions:

5.1.1-0 to 5.1.1-4 (included in System 800xA 5.1 FP4 with revisions)
6.0.0-0 to 6.0.0-2 (included in System 800xA 6.0 with revisions)
6.1.0-0 to 6.1.0-1 (included in System 800xA 6.1)

Vulnerability ID

ABB ID: ABBVU- 800xACON-OL-5114-001

Summary

On the 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public.

AC 800M uses the operating system VxWorks, but it is only affected by two of these vulnerabilities:

CVE	Title	Impact on AC 800M
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	No
CVE-2019-12255	TCP Urgent Pointer = 0 leads to integer underflow	No
CVE-2019-12260	TCP Urgent Pointer state confusion caused by malformed TCP AO option	No
CVE-2019-12261	TCP Urgent Pointer state confusion during connect() to a remote host	No
CVE-2019-12263	TCP Urgent Pointer state confusion due to race condition	No
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	No
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report	No

An attacker who successfully exploited these vulnerabilities could disrupt ongoing communication or block new communication.

References

Information from WindRiver about the VxWorks vulnerabilities is available here:
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

NVD Summary Links:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-12258 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-12262.

Information on how different ABB products are affected by the VxWorks vulnerabilities is available here:
https://new.abb.com/about/technology/cyber-security/alerts-and-notifications.
One of the documents is the Cyber Security Notification "WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation products" (document number 8VZZ001892T0001).
A Cyber Security Advisory will be issued describing the impact on the Select I/O Fieldbus Communication Interface CI845.

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.

CVSS v3 Base Score:	5.3 (Medium)
CVSS v3 Temporal Score:	5.0 (Medium)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:W/RC:C

CVSS v3 Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:W/RC:C

Recommended immediate actions

Assess the installation specific risk based on this advisory. Use the recommendations described under mitigating factors and work arounds.

It is strongly recommended to plan for an upgrade when a corrected version is available.

- No correction planned for product in limited life-cycle phase, i.e. 5.1.1-0 to 5.1.1-4 (included in System 800xA 5.1 FP4 with revisions).
- A correction is released in Control Software for AC 800M 6.0.0-3 which is part of System 800xA 6.0.3.3.
- A correction is released in Control Software for AC 800M 6.1.1-0 which is part of System 800xA 6.1.1.0.

This advisory will be updated when corrected versions are released, or otherwise relevant information becomes available.

Vulnerability Details

AC 800M uses the TCP/IP stack from the operating system VxWorks. A vulnerability exists in this TCP/IP stack in the product versions listed above. An attacker could exploit the vulnerability by sending specially crafted messages to the AC 800M controller via the Control Network, i.e. via the ports CN1 or CN2. This could disrupt ongoing TCP/IP communication on the Control Network, both for the affected

controller and for other nodes on the Control Network. Depending on which messages that are sent to the controller the communication may be just temporarily disrupted or may be persistently disturbed until a restart of the controller is performed. The type of messages that may disturb the communication persistently, can only be sent by an attacker with direct access to the Control Network. An attacker who has access to the Control Network via a router may only send the type of messages that may disrupt the communication temporarily.
Communication via other communication ports, e.g. the ModuleBus for direct IO and communication via Communication Interface Modules on AC 800M's Communication Expansion Bus (the CEX-Bus) is not affected.
The Select I/O Fieldbus Communication Interface CI845 is affected. A separate Cyber Security Advisory will be issued describing the impact on CI845.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. 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 must be evaluated case by case. Process control & automation systems should not be used for general business functions (e.g. Internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for malicious software before they are connected to a control system.

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

System 800xA 6.1 Network Configuration (3BSE034463-610).
Previous versions of this manual also contain similar recommendations, but the latest version contains more up to date recommendations that are not dependent on the used product versions.

Detection and actions in case of an attack

In case of an attack the system should be investigated so that the source of the attack can be removed. Disrupted communication will be indicated for the applications using this communication and the applications will take whatever actions they are programmed to take in such a situation.
One type of attack will only temporarily affect the controller communication and if an attacked controller automatically resumes the communication, no further actions are needed, provided that the source of the attack has been removed and potential consequences have been analyzed and responded to.
One type of attack may disturb the communication persistently. This could mean that communication connections are disrupted and cannot be automatically re-established. It could also mean that controller, from the point of view of the redundancy protocol RNRP, appears to be disconnected.
If the communication is persistently disturbed, it can only be reestablished if the controller is restarted.

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 the ports CN1 and CN2 on the Processor Module of the AC 800M controller.

What causes the vulnerability?

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

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

VxWorks is the real time operating system used by AC 800M. It includes e.g. the TCP/IP stack which is the SW component handling the AC 800M Control 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.

Can an attacker use the vulnerability to cause the AC 800M HI to take unsafe actions?

The vulnerability is a Denial of Service vulnerability. This means that an attacker may cause the controller to stop communicating, but not to take any actions that it is not programmed for. Safety measures that monitor communication will take their designed actions if communication stops. A safety application will be able to act as it is programmed to act.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating specially crafted messages and sending the message to an affected controller. For some of the messages this would require that the attacker has direct access to the Control Network. For others the attack could additionally also be done through a wrongly configured or penetrated firewall. An attack could also be done by installing malicious software on a system node or otherwise infect 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.

Is there an update that corrects the problem?

The correction removes 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 WindRiver. 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 AC 800M 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 https://new.abb.com/contact-centers.

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2019-09-23
B	P3, P5	Updated due to correction released in 800xA 6.0.3.3 and in 6.1.1.0	2021-07-02