ABB DOC ID: 2PAA120777
REVISION: B
DATE: 2020-03-17

CYBER SECURITY ADVISORY

SECURITY WindRiver VxWorks IPNet Vulnerabilities impact on CI845

Vulnerability ID: ABBVU-IACT- 800xAIOE-OL-1000-10017

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

CI845 with versions:

1.0.1.0 (included in System 800xA 6.1)

Vulnerability ID

ABB ID: ABBVU-IACT-800xAIOE-OL-1000-10017

Summary

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

CI845 uses the operating system VxWorks, but it is only affected by two of these vulnerabilities:

CVE	Title	Impact on CI845
CVE-2019-12256	Stack overflow in the parsing of IPv4 packets' IP options	Yes
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	No
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. In addition, an unconfirmed risk of Remote Code Execution exists for CI845.

References

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

National Vulnerability Database (NVD) Summary Links:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-12256
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.

From this page, the following two documents are related to this CI845 Cyber Security Advisory:
Cyber Security Notification "WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation products" (document number 8VZZ001892T0001)
Cyber Security Advisory "SECURITY WindRiver VxWorks IPNet Vulnerabilities, impact on AC 800M" (document number 2PAA120481)

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:	9.8 (Critical)
CVSS v3 Temporal Score:	8.5 (High)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R
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:H/I:H/A:H/E:P/RL:O/RC:R

Recommended immediate actions

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

The problem is corrected in CI845 versions 1.0.2.0 or later. The Firmware Upgrade Tool with CI845 version 1.0.2.0 is available in ABB Library:

Document ID	3BSE095529
Name	ABB Select IO CI845 Upgrade to 1.0.2.0
Download Link	https://search.abb.com/library/Download.aspx?DocumentID=3BSE095529&LanguageCode=en&DocumentPartId=&Action=Launch

It is strongly recommended to plan for upgrades of affected CI845 to version 1.0.2.0 using the Firmware Upgrade Tool to correct this problem. Further instructions can be found in the downloaded package within the Readme.txt file.

Vulnerability Details

CI845 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 CI845 via the Ethernet Network.

This could disrupt ongoing communication on the Ethernet Network, both for the affected module and for other participants on the network. The CI845 is disturbed until a restart of the module is performed in order to re-establish its functionality.

In addition to this confirmed risk of Denial of Service, an unconfirmed risk of Remote Code Execution exists for 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. A firewall which filters out IP packets with IP options LSRR/SSRR will prevent routed exploitation of the remote code execution vulnerability. 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)
System 800xA S800 I/O and Select I/O – Network Application Guide for Industrial Ethernet (3BSE082733)

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.
The attack may stop all CI845 modules persistently and thus stop the complete Ethernet communication persistently. This could mean that communication connections are disrupted and cannot be automatically re-established. It can only be re-established if the CI845 module is restarted. In addition to this confirmed risk of Denial of Service, an unconfirmed risk of Remote Code Execution exists for CI845.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could affect communication on the Ethernet Network, i.e. the network connected to the ports 1 and 2 of the Ethernet Adapter belonging to the affected CI845 module. In addition, there is an unconfirmed risk of Remote Code Execution for CI845.

What causes the vulnerability?

The vulnerability is caused by insufficient input data validation in the TCP/IP stack in VxWorks used by CI845.

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

VxWorks is the real time operating system used by CI845. It includes e.g. the TCP/IP stack which is the software component handling the CI845 Ethernet 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 Ethernet Network. The attacker might also be able to execute code remotely on CI845 and by this means attack the integrity of the module. Furthermore, before full disruption of communication, an attacker might cause unexpected behavior of Ethernet communication by assigning additional and colliding IP addresses to affected CI845 modules.

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 affected modules. 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 CI845 could exploit this vulnerability, but routed exploitation of the Remote Code Execution vulnerability can be prevented if the network is not connected to any external network or if it is connected using a firewall/router which filters out IP packets with IP options LSRR/SSRR.

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?

ABB verified corrections to the problem which remove the vulnerability by modifying the way that the TCP/IP stack validates messages.

These corrections are part of CI845 in versions 1.0.2.0 or later. It is strongly recommended to upgrade the CI845 to version 1.0.2.0 or later in order to correct the problem. The Firmware Upgrade Tool with CI845 version 1.0.2.0 is available in ABB Library.

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 described that CI845 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.