CYBER SECURITY NOTIFICATION – INDUSTRIAL AUTOMATION

Cyber Security Notification

WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Industrial Automation products

Release date: July 29, 2019

Update date: None (original document)

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.

Summary

On the 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public. The announcement identifies VxWorks version 6.5 and later are affected by one or more of the CVEs listed below. See LINK.

ABB Industrial Automation is evaluating the potential impact on a number of products and has initiated our vulnerability handling process to ensure any product related issues are properly addressed. With this announcement from Wind River it is understood that ABB will need to develop patches or fixes for some products to address these vulnerabilities in the VxWorks software. We are currently analyzing and planning the maintenance releases for supported ABB Industrial Automation products that utilize VxWorks. Potentially affected customers should expect additional communication or advisories as more details become available.

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-2019-12257	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc	8.8
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-2019-12261	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-2019-12259	DoS via NULL dereference in IGMP parsing	6.3
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-2019-12265	IGMP Information leak via IGMPv3 specific membership report	5.4

Affected Products

ABB Industrial Automation is still investigating the potentially affected products and to date ABB has identified the following products which are likely affected by the vulnerabilities in VxWorks (Industrial Automation products not listed are initially evaluated as not impacted):

Product Family	Products	Affected Versions
AC 800M Series	PM851/PM856/PM860/PM857/PM858/PM861/ PM862/PM863/PM864/PM865/PM866/PM867/ & PM891 Control Processors CI 845 Field Communication Interface	800xA System version 5.1.1. feature pack 4 and later. All revisions
Symphony Plus MR Series	PM 877 Controller	Revision 3.00 through 3.28
Symphony Plus SD Series	CI 850- Communications interface module for IEC-61850	Revision A_0 and A_1
UNITROL 6000	Main control channel PC D530, PP D512 for X-Power	Version 5.0.0 and higher
SYNCHROTACT 6	All products	All versions

Mitigation Factors

Recommended security practices and firewall configurations can help protect an industrial control network from attacks that originate from outside the network. Such practices include that protection, control & automation 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. In general protection, control & automation systems should not be used for general business functions which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system. Block all non-trusted IP communications.

Support

For additional information and support please contact your product provider or 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.