CYBER SECURITY NOTIFICATION

Cyber Security Notification

WindRiver VxWorks IPNet Vulnerabilities, impact on ABB Robot Controller Software

Release date: 30th of July 2019

Update date: 20th of August 2019

Summary

On the 29th of July 2019, a series of vulnerabilities from Wind River affecting the VxWorks operating system were made public by Wind River. The announcement identifies VxWorks version 6.5 (and later including up to current versions of 6.9.x and 7.x) are affected by one or more of the CVEs CVE-2019-12255 to CVE-2019-12265 which are related to TCP/IP communication. See Wind River Security Advisory for more details.

ABB Robotics is collaborating with Wind River to find the proper actions to mitigate the security risk on release products. All new releases from this date will have the updated VxWorks operating system (includes RW7 and RW 6.10).

We are currently planning the maintenance releases for supported ABB Robotics products that utilize VxWorks.   ABB Robotics will publish advisories as more details become available. Advisory is planned to be available latest end of August.

Affected Products

ABB Robotics has identified the potentially affected products and is planning/developing new releases of RobotWare:

Products and Affected Versions
RobotWare – Including RW5.6x to RW6.9.x

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.

Notice

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

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.