CYBER SECURITY NOTIFICATION

Cyber Security Notification

Wibu CodeMeter Vulnerabilities, impact on ABB products

Release date: 10.9.2020

Update date: 12.02.2021

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.

Copyright © 2021 ABB. All rights reserved.

© Copyright 2021 ABB. All rights reserved.

Summary

On the 8th of Sep 2020, a series of vulnerabilities affecting CodeMeter Runtime from WIBU SYSTEMS, were made public through WIBU security advisories web site. Products using this service might be affected by one or more of the Common Vulnerabilities and Exposures (CVEs) listed below.

ABB is evaluating the potential impacts 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 WIBU SYSTEMS it is understood that ABB will need to integrate patches or fixes to address these vulnerabilities in the CodeMeter Runtime for products which are affected, according to the ABB Vulnerability Handling policy. We are currently analyzing our product portfolio for exposure. Potentially affected customers should expect additional communication or advisories as more details become available.

The vulnerability CVE numbers and CVSS scores are listed in the table below:

CVE	CVSSv3 Score
CVE-2020-14513	7.5
CVE-2020-14519	8.1
CVE-2020-14509	10.0
CVE-2020-14517	9.4
CVE-2020-16233	7.5
CVE-2020-14515	7.4

© Copyright 2021 ABB. All rights reserved.

Affected Products

The products listed in the table are affected by the vulnerabilities listed. ABB continues to evaluate the vulnerabilities and will update the notification when additional information becomes available

Product / System line	Products and Affected Versions	Link to Advisory
Drive Application Builder	Drive Application Builder, version 1.1.0 and older	Advisory
ABB Ability™ Virtual Commissioning for drives	ABB Ability™ Virtual Commissioning for drives, version 1.0.1 and older	
ABB Ability™ Condition Monitoring for drives	ABB Ability™ Condition Monitoring for drives On-premises v 1.4 and older	
AC 800PEC platform	AC 800PEC Tool 2.6.1.0 and older EXC Control Terminal (ECT) 2.6.1.0 and older Control Terminal Management Studio (CTMS) 2.6.1.0 and older Traction Control Terminal (TCT) – "BORDLINE-View V" 2.6.1.0 and older	Advisory
Automation Studio	Automation Studio older than version 4.10	Advisory
Automation Builder	Automation Builder older than Version 2.3.0	Advisory
ABB Ability(TM) Operations Data Management zenon	ABB Ability(TM) Operations Data Management zenon, version 8.10 and older	Advisory
APROL	APROL Process Control System older than version R 4.2-06P1	Advisory
Technology Guarding	Technology Guarding older than version 1.2.1.5	Advisory
PVI Development Setup	PVI Development Setup older than version 4.10	Advisory
Automation Studio Target for Simulink	Automation Studio Target for Simulink, versions 6.0.0.x to 6.3.0.x	Advisory

© Copyright 2021 ABB. All rights reserved.

ABB products not listed are initially evaluated as not impacted. We will continue the investigation and update the table if products are identified as affected.

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 ensuring 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.

To minimize the risk of exploitation of the CodeMeter vulnerabilities users should take these defensive measures:

- Locate the control system network behind a firewall and separate them from other networks.
- In environments where CodeMeter network license server is not in use, configure firewall to block access to port TCP 22350
- Block anomalous IP traffic by utilizing a combination of firewalls and intrusion prevention systems.
- Disable or block IP tunneling, both IPv6-in-IPv4 or IP-in-IP tunneling.
- Avoid exposure of the devices to the Internet and use secure methods like VPN when accessing them remotely.

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.

© Copyright 2021 ABB. All rights reserved.