ABB DOC ID: 3ADR010770
REVISION: A
DATE: 2021-06-21

CYBER SECURITY ADVISORY

Vulnerabilities in Wibu CodeMeter, impact on Automation Builder, Drive Application Builder and Virtual Drive

ABBVREP0048-3ADR010770

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

- Automation Builder (AB) versions 2.4.1.1062 and earlier
- Drive Application Builder (DAB) versions 1.1.1.631 and earlier
- Virtual Drive version 1.0.2.105 and earlier

Vulnerability IDs

ABB ID: ABBVREP0048-3ADR010770

CVE	CVSSv3 Score
CVE-2021-20093	9.1
CVE-2021-20094	7.5

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An attacker who successfully exploited these vulnerabilities could causeWibu CodeMeter License Server to crash or in case of CVE-2021-20093 read data from heap memory.

The vulnerabilities can only be exploited when changing the default settings of Wibu CodeMeter, mainly when using Wibu CodeMeter to manage network access to licenses on a license server. However, a potential attacker must already have local access to the system.

The vulnerabilities have been closed with Wibu CodeMeter V7.21a. Wibu CodeMeter V7.21a is available for download from the Wibu website.

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.

CVE-2021-20093:

CVSS v3 base score: 9.1 (Critical)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE-2021-20094:

CVSS v3 base score: 7.5 (High)

CVSS v3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Recommended immediate actions

We recommend all users to immediately update to Wibu CodeMeter V7.21a or later (Windows 32/64-Bit version). Latest Wibu CodeMeter versions are available for public download from the Wibu website (https://www.wibu.com/support/user/user-software.html).

If for any reasons the recommended update cannot be made and if Wibu CodeMeter is not used to manage network access to licenses on a license server, ABB recommends to check that the default settings are kept, especially:

- Run CodeMeter as client only and use localhost as binding for the CodeMeter communication. With binding to localhost an attack is no longer possible via remote network connection. The network server is disabled by default.
- The CmWAN server is disabled by default. Please check if CmWAN is enabled and disable the feature.

Vulnerability Details

CVE-2021-20093

An attacker could send a specially crafted TCP/IP packet that causes the CodeMeter Runtime network server (default port 22350) to return packets containing data from the heap. When generating a response, the server copies data from a heap-based buffer to an output buffer to be sent in the response. The amount to copy is controlled by the client. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime

CVE-2021-20094

An attacker could send a specially crafted HTTP(S) request to the CodeMeter Runtime CmWAN server that causes CodeMeter Runtime Server (i.e., CodeMeter.exe) to crash. The recommended/standard setup is to run a CodeMeter Runtime CmWAN server only behind a reverse proxy with TLS and user authentication. If this is the case and the attacker is not on the same network as the CmWAN server, the attack is only possible for authenticated users. If the attacker is on the same network as the CmWAN server, an unauthenticated user can perform the attack. This is only the case if the attacker can access the CmWAN port directly (default port 22351)

Mitigating 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.

Workarounds

The vulnerabilities have been closed with Wibu CodeMeter V7.21a. Wibu CodeMeter V7.21a is available for download from the Wibu website.

It also will be integrated into the upcoming version of the affected software.

Frequently Asked Questions

What is Wibu CodeMeter for Windows?

Wibu CodeMeter for Windows is used by applications to manage licensing of these applications. The application validates the licensing of the applications on behalf of ABB. Wibu CodeMeter is installed as part of products mentioned in this document locally to users' computers.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could cause Wibu CodeMeter License Server to crash or eventually read data from heap memory

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects 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.

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.

What happens to my licenses, if I update Wibu CodeMeter Runtime?

Updating the Wibu CodeMeter Runtime version does not affect the activated licenses. All licenses that have been available prior to the update will be available after the update without taking any further actions.

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.