9AKK107991A1282 SECURITY ANNOUNCEMENT 21-01

ABB Ability™ Operations Data Management zenon

Vulnerabilities in Wibu Systems Codemeter Software components

Introduction

ABB has received a report from Wibu Systems, detailing six security vulnerabilities in the Wibu CodeMeter software.

The Wibu CodeMeter software is used for dongle licensing by the zenon editor, zenon runtime, zenon web server, zenon logic runtime.

For some versions, this software is part of the installation of these software products, even if no dongle license is being used.

On September 8th 2020, the information on these vulnerabilities was publicly available through Wibu cyber-security advisory website.

In June 2021 two further vulnerabilities were publicly available through Wibu cyber-security advisory website.

Products affected

The ABB Ability™ Operations Data Management – zenon versions 7.50, 7.60, 8.00, 8.10 are affected by these vulnerabilities.

Mitigation

Wibu Systems provides an updated version of the Codemeter software that addresses and fixes all vulnerabilities reported in this advisory.

For Zenon version 8.10 and older it is recommended to update the CodeMeter software to version 7.21a or newer. The link to the CodeMeter software update package is supplied on the ABB Ability™ Operations Data Management – zenon web page.

Vulnerability details

The report by Wibu Systems contains the following vulnerabilities. Details are provided for each vulnerability individually.

- CVE-2020-14509
- CVE-2020-14513
- CVE-2020-14515
- CVE-2020-14517
- CVE-2020-14519
- CVE-2020-16233
- CVE-2021-20093
- CVE-2021-20094

CVE-2020-14509: CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
CVSS v3 base score and vector:

- A CVSS base score of 10.0 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Remediation:
Please update the Wibu Codemeter software package.

CVE-2020- 14513: Improper Input Validation of WibuRaU files in CodeMeter Runtime
CVSS v3 base score and vector:

- A CVSS base score of 7.5 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Remediation:
Please update the Wibu Codemeter software package.

CVE-2020- 14515: Improper Signature Verification of CmActLicense update files for CmActLicense Firm Code
CVSS v3 base score and vector:

- A CVSS base score of 7.4 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H

Remediation:
Please update the Wibu Codemeter software package.

CVE-2020- 14517: CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
CVSS v3 base score and vector:

- A CVSS base score of 9.4 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Remediation:
Please update the Wibu Codemeter software package.

CVE-2020- 14519: CodeMeter Runtime WebSockets API: Missing Origin Validation
CVSS v3 base score and vector:

- A CVSS base score of 8.1 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

Remediation:
Please update the Wibu Codemeter software package.

CVE-2020- 16233: CodeMeter Runtime API: Heap Leak
CVSS v3 base score and vector:

- A CVSS base score of 7.5 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Remediation:
Please update the Wibu Codemeter software package.

CVE-2021- 20093: CodeMeter Runtime Server: Heap buffer over-read vulnerability
CVSS v3 base score and vector:

- A CVSS base score of 9.1 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Remediation:
This vulnerability cannot be exploited in the default configuration of Zenon since the CodeMeter Runtime Server is not active. Anyway, it is recommended to update the Wibu Codemeter software package.

CVE-2021- 20093: CodeMeter Runtime Server: Denial of service vulnerability
CVSS v3 base score and vector:

- A CVSS base score of 7.8 has been calculated for this vulnerability.
- The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Remediation:
This vulnerability cannot be exploited in the default configuration of Zenon since the CodeMeter Runtime Server is not active. Anyway, it is recommended to update the Wibu Codemeter software package.

Update
ABB and its suppliers recommend that system integrators and asset owners perform a risk assessment to establish whether the updated version of Wibu Codemeter software shall be installed.

Considering the criticality of the issues reported, ABB and its suppliers recommend installing the update at the earliest opportunity.

ABB and its suppliers recommend testing the updated version of the Wibu Codemeter software in a test environment to verify normal operation of the system according to project specific configuration and hardware environment, prior to installing the patch in a production environment.

ABB and its suppliers recommend that a contingency plan is in place to roll back the installation of the patch in case of any unexpected issues with the production environment following the installation of the patch.

The installer of the Wibu Codemeter software is capable of updating an existing installation. It is not required to uninstall the existing Wibu Codemeter software for Windows software first.

The installation can be started by running the downloaded installer file.

General recommendations
ABB generally recommends restricting local physical access to authorized people only. Network access shall be limit to communication that is absolutely required.

ABB further recommends using application whitelisting to restrict execution of applications to only those applications that are required for the operation of the system.

Acknowledgements
ABB wishes to thank Wibu Systems for announcing the publication of these issues to their partners, prior to the public release.

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 https://www.abb.com/cybersecurity.

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.

Version information

Date	Comment
2020-09-08	Initial Information
2020-11-11	Updated remediations to use CodeMeter 7.10a or newer
2021-09-24	Updated remediations to use CodeMeter 7.21a or newer