PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #01/2021

B&R Products affected by WIBU CodeMeter Vulnerabilities

Document Version: 1.0

First published: 2021-02-11
Last updated: N/A (Initial version)

Notice

Executive Summary

B&R is aware of six vulnerabilities in the CodeMeter Runtime software manufactured by WIBU Systems.

CodeMeter Runtime is included in the following B&R software products:

- APROL
- Technology Guarding

B&R Technology Guarding is included in the following B&R software products:

- Automation Studio
- PVI Development Setup
- Automation Studio Target for Simulink

When installing one of the software products mentioned above, CodeMeter Runtime gets installed on the target system. Installation of B&R software products containing vulnerable CodeMeter Runtime versions results in target systems affected by the vulnerabilities discussed in this advisory.

Affected Products

Product	Affected Version
APROL	All versions <R 4.2-06P1
Technology Guarding	All versions <1.2.1.5
Automation Studio	All versions <4.10
PVI Development Setup	All versions <4.10
Automation Studio Target for Simulink	Versions 6.0.0.x to 6.3.0.x

Vulnerability ID

CVE-2020-14509 CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
CVE-2020-14513 Improper Input Validation of Update Files in CodeMeter Runtime
CVE-2020-14515 Improper Signature Verification of Update Files in CodeMeter Runtime
CVE-2020-14517 CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
CVE-2020-14519 CodeMeter Runtime WebSockets API: Missing Origin Validation
CVE-2020-16233 CodeMeter Runtime API: Heap Leak

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2020-14509 CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
CVSS v3.1 Base Score: 10.0 (Critical)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-14513 Improper Input Validation of Update Files in CodeMeter Runtime
CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2020-14515 Improper Signature Verification of Update Files in CodeMeter Runtime
CVSS v3.1 Base Score: 7.4 (High)
CVSS v3.1 Vector: AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H

CVE-2020-14517 CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
CVSS v3.1 Base Score: 9.4 (Critical)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVE-2020-14519 CodeMeter Runtime WebSockets API: Missing Origin Validation
CVSS v3.1 Base Score: 8.1 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVE-2020-16233 CodeMeter Runtime API: Heap Leak
CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Corrective Actions or Resolution

WIBU Systems has closed all six vulnerabilities in CodeMeter Runtime version 7.10a.
B&R has integrated CodeMeter Runtime version 7.10b[1] into the following product versions:

Product	Corrected Version
APROL	R 4.2-06P1
Technology Guarding	1.2.1.5

A fixed Technology Guarding version has been integrated into the following product version:

Product	Corrected Version	Release Date
Automation Studio Target for Simulink	6.3.1.79	2021-01-05

[1] CodeMeter Runtime for Windows version 7.10a contained a bug in the setup routine which was fixed in version 7.10b.

A fixed Technology Guarding version will be integrated into the following upcoming product versions:

Product	Corrected Version	Planned Release Date
Automation Studio	4.10	Q2/2021
PVI Development Setup	4.10	Q2/2021

Important note:
Vulnerable CodeMeter Runtime versions installed by Automation Studio, PVI Development Setup or Automation Studio Target for Simulink can generally be upgraded to a fixed version by installing Technology Guarding 1.2.1.5 or higher on the target system.
Feasibility of such an upgrade depends on various factors like the installed version of Automation Studio, PVI Development Setup or Automation Studio Target for Simulink. In case you want to upgrade, please approach your B&R service contact.

Vulnerability Details

The CodeMeter Runtime software included in vulnerable B&R product versions is affected by six vulnerabilities. An adversary could exploit these vulnerabilities by sending a specially crafted message to affected systems. Upon receipt of that message, the systems may stop working or may become inaccessible, allowing the adversary to take control of the system or to insert and run arbitrary code on it.

For details about each vulnerability, please consult the respective security advisory published on the WIBU Security Advisories page.

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines. Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

Document History

Version	Date	Description
1.0	2021-02-10	Initial version