PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: VMT MSS and VMT IS / VMT GmbH – Several vulnerabilities in products utilizing WIBU SYSTEMS CodeMeter components

Document ID TDOCT-6967_ENG
Publication date 2020-09-09

Vulnerabilities or CVE Identifier

Identifier	WIBU Security Advisory	Vulnerability Type	Description
CVE-2020-14509	WIBU-200521-03	CWE-805: Buffer Access with Incorrect Length Value	CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
CVE-2020-14513	WIBU-200521-01	CWE-20: Improper Input Validation	Improper Input Validation of WibuRaU files in CodeMeter Runtime
CVE-2020-14515	WIBU-200521-06	CWE-347: Improper Verification of Cryptographic Signature	Improper Signature Verification of CmActLicense update files for CmActLicense Firm Code
CVE-2020-14517	WIBU-200521-04	CWE-326: Inadequate Encryption Strength	CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
CVE-2020-14519	WIBU-200521-02	CWE-346: Origin Validation Error	CodeMeter Runtime WebSockets API: Missing Origin Validation
CVE-2020-16233	WIBU-200521-05	CWE-404: Improper Resource Shutdown or Release	CodeMeter Runtime API: Heap Leak

Severity

Identifier	Base Score and Vector
CVE-2020-14509	10 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVE-2020-14513	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2020-14515	7.4 (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H)
CVE-2020-14517	9.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H)
CVE-2020-14519	8.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H)
CVE-2020-16233	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H)

Affected products

VMT GmbH:

- VMT MSS Version 1.28.1 and previous, but only if WIBU SYSTEMS CodeMeter Runtime Version lower than 7.10 is installed.
- VMT IS Version 7.x and previous, but only if WIBU SYSTEMS CodeMeter Runtime Version lower than 7.10 is installed.

Summary

Several vulnerabilities have been discovered in the utilized component WIBU SYSTEMS CodeMeter Runtime.

For detailed information please refer to WIBU SYSTEMS original Advisories at https://wibu.com/support/security-advisories.html

Impact

Pepperl+Fuchs analyzed and identified affected products.
Products are affected according to WIBU Systems classification.

Solution

For VMT MSS:

Update to WIBU Systems CodeMeter Runtime 7.10 or newer.

For VMT IS:

Please contact VMT GmbH to receive support for the product update process.

In general and without any update, this product can be operated in a secure local network that has no connection to an untrusted network, like internet or global corporate IT-net.

Reported by

Sharon Brizinov and Tal Keren of Claroty
WIBU SYSTEMS
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.