SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS

WIBU-SYSTEMS AG | Rüppurrer Straße 52-54 | 76137 Karlsruhe | Deutschland

Karlsruhe, Germany - 16 September 2020

**Important Information about CodeMeter**

Dear CodeMeter User!

The publisher of the software used by you employs CodeMeter for protection and licensing purposes. A security analyst has notified us about the presence of six vulnerabilities in CodeMeter Runtime. These have been made public on September 8th, 2020 under the following CVE identifiers:

- CVE-2020-14509: CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
  This CVE vulnerability severity rating is 'Critical' (CVSS Rating: 10.0).
  The vulnerability affects the TCP/IP communication of CodeMeter License Server. Sending manipulated packets can cause a crash of CodeMeter License Server or possibly inject and execute code.
- CVE-2020-14513: Improper Input Validation of Update Files in CodeMeter Runtime
  This CVE vulnerability severity rating is 'High' (CVSS Rating: 7.5).
  The vulnerability affects Update Files for CmActLicense Firm Codes (Firm Code 5.xxx.xxx) and provides the possibility to block CodeMeter License Server so that it no longer responds to other requests.
- CVE-2020-14515: Improper Signature Verification of Update Files in CodeMeter Runtime
  This CVE vulnerability severity rating is 'High' (CVSS Rating: 7.4).
  The vulnerability affects only Update Files for CmActLicense Firm Codes (Firm Code 5.xxx.xxx) and allows the modification of license files.
- CVE-2020-14517: CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
  This CVE vulnerability severity rating is 'Critical' (CVSS Rating: 9.4).
  The vulnerability affects the encryption and authentication of the communication between applications and CodeMeter License Server. Basically, the CodeMeter API is designed as an open API and does not provide authentication by default. If the encryption is broken, data transmitted between the application and the CodeMeter License Server can be read and manipulated.
- CVE-2020-14519: CodeMeter Runtime WebSocket API: Missing Origin Validation
  This CVE vulnerability severity rating is 'High' (CVSS Rating: 8.1).
  The vulnerability refers to a missing check on the origin of a request for the WebSocket API and allows the modification of license files. The WebSocket API is usually used exclusively for direct activation in License Central WebDepot and can be deactivated. Deactivation is especially recommended if CodeMeter prior to version 6.90 is used and cannot be updated.
- CVE-2020-16233: CodeMeter Runtime API: Heap Leak
  This CVE vulnerability severity rating is 'High' (CVSS Rating: 7.5).
  The vulnerability affects CodeMeter License Server and allows reading of data from heap memory by sending specially manipulated requests.



**WIBU-SYSTEMS AG | Deutschland**
Rüppurrer Straße 52-54 | D-76137 Karlsruhe
Telefon: +49-721-93172-0 | Fax: +49-721-93172-22
E-Mail: info@wibu.com | www.wibu.com
USt-ID: DE 143606433 | WEEE-Reg-Nr: DE 90465365

**Vorstand**
Dipl.-Ing. Oliver Winzenried
**Aufsichtsratsvorsitzender**
Dipl.-Inform. Marcellus Buchheit
HRB 107315 | Amtsgericht Mannheim

**Bankverbindungen**
Baden-Württembergische Bank
Deutsche Postbank AG
Commerzbank AG
vormals Dresdner Bank

**IBAN**
DE87 6005 0101 0008 0239 79
DE88 6601 0075 0005 5167 52
DE08 6608 0052 0609 0060 00

**Swift | BIC**
SOLADEST600
PBNKDEFF660
DRESDEFF660

**EORI**
DE2670844

WIBU-SYSTEMS AG | Rüppurrer Straße 52-54 | 76137 Karlsruhe | Deutschland

After these vulnerabilities were reported to us, we immediately evaluated them, researched the causes and eliminated them. A detailed overview of the respective vulnerabilities can be found in the corresponding Security Advisories, which you can download at https://wibu.com/support/security-advisories.html. There you can also see which vulnerabilities have been fixed in which versions and which countermeasures can be taken for systems that have not yet been or cannot be updated.

Due to the classification of the vulnerabilities, we strongly recommend – especially for systems not running in secured environments – an update of the CodeMeter runtime to the version 7.10a.

The version CodeMeter 7.10a is available for download at
https://www.wibu.com/support/user/user-software.html

***Frequently Asked Questions:***

***Q:*** How critical is the situation in practice?
***A:*** In order to exploit the vulnerabilities, attackers must either have access to the system itself or access to a system on the same network. Attackers must have already broken into the network or gained access to it. If they have managed to do so, they can exploit the specified vulnerabilities. However, one of the vulnerabilities (CVE-2020-14519) can be exploited just by calling up an appropriately prepared web page.

***Q:*** Do I have to install the update on all systems?
***A:*** The CodeMeter Runtime on all platforms (Windows, macOS, Linux) is affected.

***Q:*** My systems are running in a protected environment. Do I still have to install the update?
***A:*** If you can make sure that attackers cannot gain access to your network and only Update Files from trusted sources are processed, then the vulnerabilities cannot be exploited and you can do without the update. If it is possible to access websites on the Internet from this computer, you should deactivate access to the WebSocket API for security reasons (see below).

***WebSocket API***

***Q*:** What is the WebSocket API used for and by whom?
***A*:** The WebSocket API allows you to query information about existing CmContainers from a web browser, create Context Files and import Update Files. It is usually only used by CodeMeter License Central WebDepot.
The Software Activation Wizard that uses the CodeMeter License Central Gateways and the file-based activation in CodeMeter License Central WebDepot are **not** using WebSocket API

***Q:*** How does CodeMeter License Central WebDepot behave if the WebSocket API is disabled or cannot be loaded due to incompatibility?
***A:*** If WebDepot cannot successfully communicate with the WebSocket API, it automatically switches to file-based activation. In this case, users have to create the Context Files and apply downloaded



**WIBU-SYSTEMS AG | Deutschland**
Rüppurrer Straße 52-54 | D-76137 Karlsruhe
Telefon: +49-721-93172-0 | Fax: +49-721-93172-22
E-Mail: info@wibu.com | www.wibu.com
USt-ID: DE 143606433 | WEEE-Reg-Nr: DE 90465365

**Vorstand**
Dipl.-Ing. Oliver Winzenried
**Aufsichtsratsvorsitzender**
Dipl.-Inform. Marcellus Buchheit
HRB 107315 | Amtsgericht Mannheim

**Bankverbindungen**
Baden-Württembergische Bank
Deutsche Postbank AG
Commerzbank AG
vormals Dresdner Bank

**IBAN**
DE87 6005 0101 0008 0239 79
DE88 6601 0075 0005 5167 52
DE08 6608 0052 0609 0060 00

**Swift | BIC**
SOLADEST600
PBNKDEFF660
DRESDEFF660

**EORI**
DE2670844

WIBU-SYSTEMS AG | Rüppurrer Straße 52-54 | 76137 Karlsruhe | Deutschland

Update Files themselves. In principle, however, all actions are also possible with the file-based activation.

***Q:*** What are the new features of the new WebSocket API in CodeMeter version 7.10a?
***A:*** The new version of the WebSocket API requires the use of a certificate issued by Wibu-Systems for the website that wants to exchange information and data with CodeMeter License Server. The previous version of the WebSocket API is deactivated by default.
This means that a CodeMeter runtime environment version 7.10a can only perform direct activation with an appropriately updated WebDepot.

***Q:*** How can I reactivate the old WebSocket API for CodeMeter version 7.10a?
***A:*** By setting the profiling entry 'CmWebSocketAllowWithoutOriginCheck' to the value '1' and restarting CodeMeter License Server, the old WebSocket API can be reactivated without origin check. This allows you to perform a direct activation despite using an old CodeMeter License Central WebDepot.
Activating the old WebSocket API **is not recommended**. Please update CodeMeter License Central WebDepot.

***Q:*** How can the old WebSocket API be switched off and what are the effects?
***A:*** By setting the profiling entry 'CmWebSocketApi' to the value '0' and restarting of CodeMeter LIcense Server, the old WebSocket API can be deactivated.
Deactivating the WebSocket API applies **only** to the old WebSocket API version without origin verification. Once you install version 7.10a, the new WebSocket API with origin verification is available and enabled.
Deactivation is especially recommended if CodeMeter prior to version 6.90 is used and cannot be updated.
Disabling WebSocket API means that direct activation in CodeMeter License Central WebDepot can no longer be used until CodeMeter Runtime has been updated to version 7.10a or newer. The Software Activation Wizard that uses the CodeMeter License Central Gateways and the file-based activation in CodeMeter License Central WebDepot will still work.

***Q:*** If I now deactivate the WebSocket API for an older CodeMeter version previous to 7.10a, will it be reactivated by updating to a new version?
***A:*** Yes, the deactivation only is permanent for the old WebSockt API without origin verification. After updating to CodeMeter version 7.10a or later, the new WebSocket API with origin verification is immediately available.

Please accept our apologies for any inconvenience we may have caused you!

Sincerely yours,

Wolfgang Voelker
Director Product Management



**WIBU-SYSTEMS AG | Deutschland**
Rüppurrer Straße 52-54 | D-76137 Karlsruhe
Telefon: +49-721-93172-0 | Fax: +49-721-93172-22
E-Mail: info@wibu.com | www.wibu.com
USt-ID: DE 143606433 | WEEE-Reg-Nr: DE 90465365

**Vorstand**
Dipl.-Ing. Oliver Winzenried
**Aufsichtsratsvorsitzender**
Dipl.-Inform. Marcellus Buchheit
HRB 107315 | Amtsgericht Mannheim

**Bankverbindungen**
Baden-Württembergische Bank
Deutsche Postbank AG
Commerzbank AG
vormals Dresdner Bank

**IBAN**
DE87 6005 0101 0008 0239 79
DE88 6601 0075 0005 5167 52
DE08 6608 0052 0609 0060 00

**Swift | BIC**
SOLADEST600
PBNKDEFF660
DRESDEFF660

**EORI**
DE2670844