SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS

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

Karlsruhe, 16. September 2020

Wichtige Information zu CodeMeter

Sehr geehrte CodeMeter-Anwender,

für die von Ihnen eingesetzte Software nutzt der Hersteller CodeMeter zum Schutz und zur Lizenzierung. Für CodeMeter sind uns von einem Sicherheitsdienstleister sechs Schwachstellen gemeldet worden. Diese wurden am 08.09.2020 unter den nachfolgenden Nummern veröffentlicht:

- CVE-2020-14509: CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value
  Dieser CVE ist als Schwachstelle mit Schweregrad Kritisch (CVSS Rating: 10,0) eingestuft worden.
  Die Schwachstelle betrifft die TCP/IP-Kommunikation des CodeMeter Lizenzservers. Durch das Senden von manipulierten Paketen kann ein Absturz des CodeMeter Lizenzservers herbeigeführt oder eventuell auch Code eingeschleust und ausgeführt werden.
- CVE-2020-14513: Improper Input Validation of Update Files in CodeMeter Runtime
  Dieser CVE ist als Schwachstelle mit Schweregrad Hoch (CVSS Rating: 7,5) eingestuft worden.
  Die Schwachstelle betrifft Update-Dateien für CmActLicense Firm Codes (Firm Code 5.xxx.xxx) und ermöglicht das Blockieren des CodeMeter Lizenzservers, so dass er nicht mehr auf andere Anfragen reagiert.
- CVE-2020-14515: Improper Signature Verification of Update Files in CodeMeter Runtime
  Dieser CVE ist als Schwachstelle mit Schweregrad Hoch (CVSS Rating: 7,4) eingestuft worden.
  Die Schwachstelle betrifft nur Update-Dateien für CmActLicense Firm Codes (Firm Code 5.xxx.xxx) und ermöglicht die Modifikation von Lizenzdateien.
- CVE-2020-14517: CodeMeter Runtime API: Inadequate Encryption Strength and Authentication
  Dieser CVE ist als Schwachstelle mit Schweregrad Kritisch (CVSS Rating: 9,4) eingestuft worden.
  Die Schwachstelle betrifft die Verschlüsselung und Authentifizierung der Kommunikation zwischen Applikationen und CodeMeter Lizenzservern. Grundsätzlich ist das CodeMeter API als offenes API designed und sieht standardmäßig keine Authentifizierung vor. Durch ein mögliches Brechen der Verschlüsselung können zwischen Applikation und CodeMeter Lizenzserver übermittelte Daten mitgelesen und manipuliert werden.
- CVE-2020-14519: CodeMeter Runtime WebSocket API: Missing Origin Validation
  Dieser CVE ist als Schwachstelle mit Schweregrad Hoch (CVSS Rating: 8,1) eingestuft worden.
  Die Schwachstelle betrifft eine fehlende Prüfung auf die Herkunft einer Anfrage für das CodeMeter WebSocket API und ermöglicht die Modifikation von Lizenzdateien. Das WebSocket API wird in der Regel ausschließlich für die direkte Aktivierung im CodeMeter License Central WebDepot verwendet und kann deaktiviert werden. Eine Deaktivierung wird insbesondere empfohlen, wenn die CodeMeter Version kleiner 6.90 verwendet wird und nicht aktualisiert werden kann.
- CVE-2020-16233: CodeMeter Runtime API: Heap Leak
  Dieser CVE ist als Schwachstelle mit Schweregrad Hoch (CVSS Rating: 7,5) eingestuft worden.
  Die Schwachstelle betrifft den CodeMeter Lizenzserver und ermöglicht das Auslesen von Daten des Heap-Speichers durch das Senden von speziell manipulierten Anfragen.

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

Nachdem uns diese Schwachstellen gemeldet wurden, haben wir diese umgehend bewertet, die Ursachen erforscht und behoben. Eine detaillierte Übersicht über die gefundenen Schwachstellen finden Sie in den zugehörigen Security Advisories, die Sie unter https://www.wibu.com/de/support/security-advisories.html abrufen können. Dort ist ebenfalls ersichtlich, welche Schwachstellen in welchen Versionen behoben wurden und welche Abwehrmaßnahmen für Systeme getroffen werden können, die noch nicht aktualisiert wurden oder nicht aktualisiert werden können.

Aufgrund der Einstufung der Schwachstellen empfehlen wir – insbesondere für Systeme, die nicht in abgesicherten Umgebungen laufen, – dringend ein Update der CodeMeter Laufzeitumgebung auf die Version 7.10a.

Die Version CodeMeter 7.10a steht zum Download unter https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html zur Verfügung.

Häufig gestellte Fragen:

Frage: Wie hoch ist die Gefahr wirklich?
Antwort: Um die Schwachstellen ausnutzen zu können, muss ein Angreifer entweder Zugriff auf das System selbst oder Zugriff auf ein System im selben Netzwerk haben. Der Angreifer muss also schon in das Netzwerk eingebrochen sein oder sich dort Zugang verschafft haben. Wenn er dies geschafft hat, kann er die angegebenen Sicherheitslücken ausnutzen.
Eine der Schwachstellen (CVE-2020-14519) kann allerdings schon durch den Aufruf einer entsprechend präparierten Webseite ausgenutzt werden.

Frage: Muss ich das Update auf allen Systemen einspielen?
Antwort: Es ist die CodeMeter Laufzeitumgebung (CodeMeter Runtime) auf allen Plattformen betroffen (Windows, macOS, Linux).

Frage: Meine Systeme laufen in einer abgesicherten Umgebung. Muss ich trotzdem das Update einspielen?
Antwort: Wenn Sie sicherstellen können, dass Angreifer nicht in Ihrem Netzwerk Zugriff erlangen können und nur Update-Dateien von vertrauenswürdigen Stellen verarbeitet werden, dann können die Schwachstellen nicht ausgenutzt werden und Sie könnten auf das Update verzichten. Wenn es von diesem Rechner möglich ist, Webseiten im Internet abzurufen, sollten Sie den Zugriff auf das WebSocket API sicherheitshalber deaktivieren (siehe unten).

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

WebSocket API

Frage: Wofür und durch wen wird das WebSocket API verwendet?
Antwort: Das WebSocket API ermöglicht aus einem Webbrowser die Abfrage von Informationen über vorhandene CmContainer, das Erstellen von Context-Dateien und das Einspielen von Update-Dateien. Es wird üblicherweise ausschließlich durch das CodeMeter License Central WebDepot verwendet.

Frage: Wie verhält sich das CodeMeter License Central WebDepot, wenn das WebSocket API deaktiviert ist oder wegen Inkompatibilität nicht geladen werden kann?
Antwort: Kann das WebDepot nicht oder nicht erfolgreich mit dem WebSocket API kommunizieren, so wird automatisch auf die dateibasierte Aktivierung gewechselt. Bei dieser muss der Anwender die Context-Dateien selbst erstellen und heruntergeladene Update-Dateien selbst anwenden. Prinzipiell sind aber alle Aktionen ebenfalls mit der dateibasierten Aktivierung möglich.

Frage: Was sind die Neuerungen des neuen WebSocket APIs in CodeMeter 7.10a?
Antwort: Die neue Version des WebSocket API verlangt zwingend die Verwendung eines durch Wibu-Systems ausgestellten Zertifikats für die Website, die mit dem CodeMeter Lizenzserver Informationen und Daten austauschen möchte. Die bisherige Version des WebSocket API wird standardmäßig deaktiviert.

Frage: Wie kann ich für CodeMeter 7.10a das alte WebSocket API wieder aktivieren?
Antwort: Durch Setzen des Profiling-Eintrags 'CmWebSocketAllowWithoutOriginCheck' auf den Wert '1' kann nach einem CodeMeter Lizenzserver Neustart das alte WebSocket API ohne Origin-Prüfung wieder aktiviert werden. Damit kann ich trotz eines alten CodeMeter License Central WebDepots eine direkte Aktivierung durchführen.
Die Aktivierung des alten WebSocket API wird **ausdrücklich nicht empfohlen**.

Frage: Wie kann das bisherige WebSocket API abgeschaltet werden und welche Auswirkungen hat das?
Antwort: Durch das Setzen des Profiling-Eintrags 'CmWebSocketApi' auf den Wert '0' und einen anschließenden Neustart des CodeMeter Lizenzservers kann das bisherige WebSocket API deaktiviert werden.
Das Abschalten des WebSocket APIs gilt nur für die bisherige WebSocket API Version ohne Origin-Prüfung. Sobald man die Version 7.10a installiert, ist das neue WebSocket API mit Origin-Prüfung verfügbar und aktiviert.
Das Abschalten des bisherigen WebSocket APIs wird insbesondere empfohlen, wenn eine CodeMeter Version kleiner 6.90 verwendet wird und nicht aktualisiert werden kann.
Durch das Abschalten des bisherigen WebSocket APIs kann die direkte Aktivierung im CodeMeter License Central WebDepot solange nicht mehr verwendet werden, bis die CodeMeter Laufzeitumgebung auf Version 7.10a aktualisiert wurde.

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

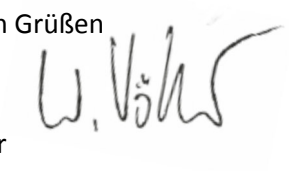
WIBU-SYSTEMS AG | Rüppurrer Straße 52-54 | 76137 Karlsruhe | Deutschland

Frage: Wie kann das bisherige WebSocket API abgeschaltet werden und welche Auswirkungen hat das?
Antwort: Durch das Setzen des Profiling-Eintrags 'CmWebSocketApi' auf den Wert '0' und einen anschließenden Neustart des CodeMeter Lizenzservers kann das bisherige WebSocket API deaktiviert werden.
Das Abschalten des WebSocket APIs gilt nur für die bisherige WebSocket API Version ohne Origin-Prüfung. Sobald man die Version 7.10a installiert, ist das neue WebSocket API mit Origin-Prüfung verfügbar und aktiviert.
Das Abschalten des bisherigen WebSocket APIs wird insbesondere empfohlen, wenn eine CodeMeter Version kleiner 6.90 verwendet wird und nicht aktualisiert werden kann.
Durch das Abschalten des bisherigen WebSocket APIs kann die direkte Aktivierung im CodeMeter License Central WebDepot solange nicht mehr verwendet werden, bis die CodeMeter Laufzeitumgebung auf Version 7.10a aktualisiert wurde.

Frage: Wenn ich für eine ältere CodeMeter Version kleiner 7.10a jetzt das WebSocket API deaktiviere, werden diese dann durch ein Update auf eine neue Version wieder aktiviert?
Antwort: Ja, denn es werden nur die WebSockets ohne Origin-Prüfung abgeschaltet. Nach einem Update auf eine CodeMeter Version 7.10a oder neuer steht das neue WebSocket API mit Origin-Prüfung sofort zur Verfügung.

Wir bitten die Unannehmlichkeiten zu entschuldigen.

Mit freundlichen Grüßen



Wolfgang Völker
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