SSA-455843: WIBU Systems CodeMeter Runtime Vulnerabilities in Siemens Products

Publication Date: 2020-09-08
Last Update: 2022-02-17
Current Version: V1.7
CVSS v3.1 Base Score: 10.0

SUMMARY

CISA and WIBU Systems disclosed six vulnerabilities in different versions of CodeMeter Runtime, a product provided by WIBU Systems and used in several Siemens products for license management.

The vulnerabilities are described in the section “Vulnerability Classification” below and got assigned the CVE IDs CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, and CVE-2020-16233. Successful exploitation of these vulnerabilities could allow an attacker to alter and forge a license file, cause a denial-of-service condition, attain remote code execution, or prevent normal operation of the Siemens software that depends on CodeMeter Runtime.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PSS CAPE Protection Simulation Platform: CAPE 14 installations installed from material dated earlier than 2020-09-15	CAPE 14 installations installed from material dated 2020-09-15 or later are not affected, as they contain a fixed version of CodeMeter Runtime If CAPE 14 was initially installed using earlier material, see the recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SICAM 230: All versions	Currently no remediation is planned Update to SICAM 230 V8.00 or later version. Install WIBU Systems CodeMeter Runtime V7.10a to fix all issues See also the recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SIMATIC Information Server 2019: Version 2019 SP1 only affected by CVE-2020-14509, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233	Update to Information Server 2019 SP1 Update 1 contained in PCS neo V3.0 SP1 Update 1 https://support.industry.siemens.com/cs/ww/en/view/109784449/ See further recommendations from section Workarounds and Mitigations

SIMATIC PCS neo: All versions < V3.0 SP1 Update 1	Update to V3.0 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109784449/ See further recommendations from section Workarounds and Mitigations
SIMATIC Process Historian 2019 (incl. Process Historian OPC UA Server): All versions < SP1 Update 1	Update to Process Historian 2019 SP1 Update 1 contained in PCS neo V3.0 SP1 Update 1 https://support.industry.siemens.com/cs/ww/en/view/109784449/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA: All versions < V3.17 P007 only affected by CVE-2020-14509, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233	Update to V3.17 P007 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMIT Simulation Platform: All versions >= V10.0 and < V10.2 Upd1	Update to V10.2 Upd1 or later version https://support.industry.siemens.com/cs/ww/en/view/109794248/ For earlier versions see the recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SINEC INS: All versions < V1.0 SP1 only affected by CVE-2020-14509, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233	Update to V1.0 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109793469/ For earlier versions see the recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations
SINEMA Remote Connect: All versions < V3.0 only affected by CVE-2020-14513, CVE-2020-14515, CVE-2020-14519	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109793790/ For earlier versions see the recommendations from section Workarounds and Mitigations See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- All products affected by CVE-2020-14513 or CVE-2020-14515: Do not import license files from untrusted sources.
- SIMATIC WinCC OA V3.17:

  Update to V3.17 P007 or later version to fix all issues. For patch levels < P007, the following measures apply:

  CVE-2020-14509, CVE-2020-14517, and CVE-2020-16233 are already mitigated by default, as no external connections to port 22350/tcp are allowed. Additionally, an update to SIMATIC WinCC OA

version V3.17 P006 partially fixes CVE-2020-14517.

CVE-2020-14519: Disable the WebSockets API of CodeMeter Runtime.

- SIMIT Simulation Platform (Versions >= V10.0 and < V10.2 Upd1):

  To fix all issues for existing installations, update CodeMeter Runtime to V7.10a: Download from the WIBU Systems User Software website and install on the SIMIT system.

- SINEC INS (Versions < V1.0 SP1 only):

  Update CodeMeter Runtime to V7.10a: Download the package "CodeMeter User Runtime for Linux, version 7.10a, Driver-only" from the WIBU Systems User Software website. Install it on the system which runs SINEC INS by executing the following command:

  ```
  sudo dpkg --force-depends --force-confnew -i codemeter-lite_7.10.4196.501_amd64.deb
  ```

- PSS CAPE Protection Simulation Platform (if initally installed from material dated earlier than 2020-09-15):

  Update CodeMeter Runtime to V7.10a: Download the package from https://www.psscape.com/codemeter and install it the same way as previous versions documented in the PSS CAPE 14 Installation Manual.

  Contact PSS®CAPE Support at psscape.support.energy@siemens.com if you need assistance with patching affected systems.

- SICAM 230

  To fix all issues for existing installations, update SICAM 230 to V8.00 or later version. Then update CodeMeter Runtime to V7.10a: Download the package from WIBU Systems User Software website. Install it on SICAM 230 systems according to the procedure documented in chapter 9 of COPA-DATA Security Vulnerability Announcement 2020_1.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

PSS(R)CAPE is a highly detailed protection simulation software for transmission and distribution networks. It supports the system protection function within electric power utilities.

SICAM 230 is a scalable process control system for a broad range of applications and can be used from an integrated energy system for utility companies to a monitoring system for smart grid applications.

SIMATIC Information Server is used to report and visualize process data stored in the SIMATIC Process Historian.

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC Process Historian is the long term archive system for SIMATIC PCS 7, SIMATIC WinCC and SIMATIC PCS neo. It stores process values, alarms and batch data of production plants in its database and offers historical process data to reporting and visualization applications.

SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SIMIT Simluation Platform allows the simulation of plant setups in order to anticipate faults in the early planning phase.

SINEC INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial networks.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2020-14509

Multiple memory corruption vulnerabilities exist where the packet parser mechanism does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-805: Buffer Access with Incorrect Length Value

Vulnerability CVE-2020-14513

CodeMeter and the software using it may crash while processing a specifically crafted license file due to unverified length fields.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-14515

There is an issue in the license-file signature checking mechanism, which could allow attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-347: Improper Verification of Cryptographic Signature

Vulnerability CVE-2020-14517

Protocol encryption can be easily broken and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

CVSS v3.1 Base Score	9.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2020-14519

This vulnerability could allow an attacker to use an internal API via a specifically crafted Java Script payload, which may allow alteration or creation of license files.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-346: Origin Validation Error

Vulnerability CVE-2020-16233

An attacker could send a specially crafted packet that could have the server send back packets containing data from the heap.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-404: Improper Resource Shutdown or Release

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts
- Bundesamt für Sicherheit in der Informationstechnik (BSI) for coordination efforts
- WIBU Systems CERT for coordination efforts

ADDITIONAL INFORMATION

For more details regarding the vulnerabilities in CodeMeter Runtime refer to:

- CISA Industrial Control Systems Advisory ICSA-20-203-01: https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01
- WIBU Systems Security Advisories: https://www.wibu.com/support/security-advisories.html
- WIBU Systems CodeMeter Runtime: https://www.wibu.com/products/codemeter/runtime.html
- WIBU Systems User Software: https://www.wibu.com/support/user/user-software.html

- COPA-DATA Security Vulnerability Announcement 2020_1: https://www.copadata.com/fileadmin/user_upload/faq/files/CD_SVA_2020_1.pdf

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-09-08):	Publication Date
V1.1 (2020-10-13):	Added PSS CAPE Protection Simulation Platform; added solution by software update for SIMATIC WinCC OA; added solution by installation of latest CodeMeter Runtime version for SIMIT, SINEC INS, and PSS CAPE
V1.2 (2020-11-10):	Added SICAM 230
V1.3 (2021-01-12):	Updated solutions for PCS neo and SPPA T3000 (with fixes for the open CVEs)
V1.4 (2021-02-09):	Updated solution for SPPA S3000 (with fixes for the open CVEs)
V1.5 (2021-03-09):	Updated solution for SINEC INS and SINEMA Remote Connect
V1.6 (2021-04-13):	Updated solution for PSS CAPE and SIMIT
V1.7 (2022-02-17):	Moved products from Siemens Energy to separate advisory SSA-455844

TERMS OF USE