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

Publication Date: 2020-09-08
Last Update: 2020-09-08
Current Version: V1.0
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 and Siemens Energy 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 is working on software updates for affected products and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Information Server: 2019 SP1 and later versions only affected by CVE-2020-14509, CVE-2020-16233, CVE-2020-14517, CVE-2020-14519	See recommendations from section Workarounds and Mitigations
Process Historian (incl. Process Historian OPC UA Server): 2019 and later versions	Update to 2019 SP1 to fix CVE-2020-14513 and CVE-2020-14515 See also the recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions	Update to V3.0 SP1 to fix CVE-2020-14513 and CVE-2020-14515 See also the recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA: V3.17 only affected by CVE-2020-14509, CVE-2020-16233, CVE-2020-14517, CVE-2020-14519	See recommendations from section Workarounds and Mitigations
SIMIT Simulation Platform: V10.0 and later versions	Update to V10.2 to fix CVE-2020-14513 and CVE-2020-14515 See also the recommendations from section Workarounds and Mitigations
SINEC INS: All versions only affected by CVE-2020-14509, CVE-2020-16233, CVE-2020-14517, CVE-2020-14519	See recommendations from section Workarounds and Mitigations

SINEMA Remote Connect: All versions only affected by CVE-2020-14513, CVE-2020-14515, CVE-2020-14519	See recommendations from section Workarounds and Mitigations
SPPA-S2000 (S7): V3.04, V3.06	See recommendations from section Workarounds and Mitigations
SPPA-S3000: V3.04, V3.05	See recommendations from section Workarounds and Mitigations
SPPA-T3000: R8.2 SP2	See 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 PCS neo:

  Update to V3.0 SP1, to limit the impact of CVE-2020-14509, CVE-2020-14517, and CVE-2020-16233 to the Engineering Server only.
- SIMATIC WinCC OA:

  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.
- SINEC INS:

  To fix CVE-2020-14509, CVE-2020-16233: Download the package “CodeMeter User Runtime for Linux, version 7.10” from the WIBU Systems website and install it on the system which runs SINEC INS. This will update CodeMeter Runtime from version 6.90 to 7.10.
- SPPA-S2000 (S7), SPPA-S3000 (V3.04 only), and SPPA-T3000:

  To mitigate CVE-2020-14509, CVE-2020-14513, CVE-2020-14517, and CVE-2020-16233: Run CodeMeter only as client and use localhost as binding for the CodeMeter. I.e., prohibit external connections to port 22350/tcp on the system where CodeMeter runs.

  This mitigation measure cannot be applied to SPPA-S3000 V3.05.

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

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

Process Historian is a long term archive for process data from SIMATIC PCS neo.

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

The client-server HMI (human machine interface) system 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.

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

The software 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 ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

SPPA-S2000 emulates the automation components (S7) of the Nuclear DCS system SPPA-T2000. Together with SPPA-T2000 HMI components and a process model it represents the training simulator for SPPA-T2000.

SPPA-S3000 emulates the automation components of the DCS system SPPA-T3000. Together with SPPA-T3000 HMI components and a process model it represents the training simulator for SPPA-T3000.

SPPA-T3000 is a distributed control system mostly used in fossil and large scale renewable power plants.

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:

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

ADDITIONAL INFORMATION

The advisory covers products from both Siemens and Siemens Energy. For better readability we use the term “Siemens” to address both companies.

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

- CISA Industrial Control Systems Advisory ICSA-20-203-01
- WIBU Systems Security Advisories
- WIBU Systems CodeMeter Runtime

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

TERMS OF USE