SSA-455844: WIBU Systems CodeMeter Runtime Vulnerabilities in Siemens Energy Products

Publication Date: 2022-02-17
Last Update: 2022-02-17
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

Note: This advisory does not address new vulnerabilities. It is a clone from SSA-455843, initially published on 2020-09-08. SSA-455843 now covers Siemens products, while SSA-455844 covers Siemens Energy products.

CISA and WIBU Systems disclosed six vulnerabilities in different versions of CodeMeter Runtime, a product provided by WIBU Systems and used in several 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 Energy software that depends on CodeMeter Runtime.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SPPA-S2000 (S7): V3.04, V3.06	Apply Patch V3.06P1 See download link in the SPPA-S2000 Technical News 2021-001 See further recommendations from section Workarounds and Mitigations
SPPA-S3000: V3.04	Apply Patch V3.04P6 See download link in SPPA-S3000 Technical News 2020-004 See further recommendations from section Workarounds and Mitigations
SPPA-S3000: V3.05	Apply Patch V3.05P3 See download link in SPPA-S3000 Technical News 2020-003 See further recommendations from section Workarounds and Mitigations
SPPA-T3000: R8.2 SP2	Apply System Software Patch 19.017.20 See download link in SPPA-T3000 Technical News 2020-091 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.
- SPPA-S2000 (S7) (V3.04 and V3.06 without Patch P1), SPPA-S3000 (V3.04 without Patch P6), and SPPA-T3000 (R8.2 SP2 without System Software Patch 19.017.20):

  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. Apply V3.05P3 instead.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens Energy strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens Energy strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens Energy strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

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

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

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 (2022-02-17): Publication Date

TERMS OF USE