SSA-675303: WIBU Systems CodeMeter Runtime Vulnerabilities in Siemens Products

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 9.1

SUMMARY

WIBU Systems disclosed two vulnerabilities and a new release version 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-2021-20093 and CVE-2021-20094. Successful exploitation of these vulnerabilities could allow an attacker to read data from the heap of the CodeMeter Runtime network server, or crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

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 2021-06-16	CAPE 14 installations installed from material dated 2021-06-16 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
SICAM 230: All versions	See also the recommendations from section Workarounds and Mitigations Update to SICAM 230 V8.00 or later version. Then install WIBU Systems CodeMeter Runtime V7.21a to fix the issues.
SIMATIC Information Server: All versions >= 2019 SP1 only affected by CVE-2021-20093	See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions only affected by CVE-2021-20093	See recommendations from section Workarounds and Mitigations
SIMATIC Process Historian (incl. Process Historian OPC UA Server): All versions >= 2019 only affected by CVE-2021-20093	See recommendations from section Workarounds and Mitigations

SIMATIC WinCC OA V3.17: All versions < V3.17 P013 only affected by CVE-2021-20093	Update to V3.17 P013 or later version https://www.winccoa.com/downloads/ (login required)
SIMATIC WinCC OA V3.18: All versions < V3.18 P002 only affected by CVE-2021-20093	Update to V3.18 P002 or later version https://www.winccoa.com/downloads/ (login required)
SIMIT Simulation Platform: All versions >= V10.0 only affected by CVE-2021-20093	See recommendations from section Workarounds and Mitigations
SINEC INS: All versions only affected by CVE-2021-20093	See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions only affected by CVE-2021-20093	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:

- PSS CAPE Protection Simulation Platform (if initally installed from material dated earlier than 2021-06-16):

  Update CodeMeter Runtime to V7.21a: 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.

  Note: Installations of PSS CAPE are only affected if network access to CodeMeter Runtime is enabled. This is not the default configuration and is not necessary for any functionality in PSS CAPE.

- SICAM 230:

  To fix all issues for existing installations, update SICAM 230 to V8.00 or later version. Then update CodeMeter Runtime to V7.21a: Download the package from WIBU Systems User Software website. Install it on SICAM 230 systems according to the procedure documented in chapter 9.2 of COPA-DATA Security Vulnerability Announcement 2021_1.

- SIMATIC PCS neo, Information Server, Process Historian:

  Limit remote access to port 22350/tcp on systems where the Codemeter runtime network server is running.

- SIMATIC WinCC OA:

  For unpatched systems, limit remote access to port 22350/tcp on systems where the Codemeter runtime network server is running (for details refer to the updated security manual of WinCC OA).

- SIMIT Simulation Platform:

  To fix all issues for existing installations, update CodeMeter Runtime to V7.21a: Download from the WIBU Systems User Software website and install on the SIMIT system.

- SINEC INS:

Update CodeMeter Runtime to V7.21a: Download the package “CodeMeter User Runtime for Linux, version 7.21a, 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_7.21.4611.501_amd64.deb
```

For unpatched systems, limit remote access to port 22350/tcp on systems where the Codemeter runtime network server is running. Note that this is the default configuration, which therefore limits the exploitability to local attacks only.

- SINEMA Remote Connect Server:

  Limit remote access to port 22350/tcp on systems where the Codemeter runtime network server is running. Note that this is the default configuration, which therefore limits the exploitability to local attacks only.

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

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

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

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.

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 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.

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.

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-2021-20094

A buffer over-read vulnerability in the HTTP(S) service of the CodeMeter Runtime CmWAN server could cause the server to crash.

An unauthenticated remote attacker with access to the CmWAN port could exploit this issue to crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

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-126: Buffer Over-read

Vulnerability CVE-2021-20093

A buffer over-read vulnerability in the CodeMeter Runtime network server could cause the server to return packets containing data from the heap.

An unauthenticated remote attacker could exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-126: Buffer Over-read

ADDITIONAL INFORMATION

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

- WIBU Systems Security Advisories: https://www.wibu.com/support/security-advisories.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 (2021-07-13): Publication Date

TERMS OF USE