

SSA-580693: WIBU Systems CodeMeter Runtime Denial-of-Service Vulnerability in Siemens Products

Publication Date: 2021-11-09
 Last Update: 2021-11-09
 Current Version: V1.0
 CVSS v3.1 Base Score: 7.1

SUMMARY

WIBU Systems published information about a denial-of-service vulnerability and an associated fix release version of CodeMeter Runtime, a product provided by WIBU Systems and used in several Siemens products for license management.

The vulnerability is described in the section “Vulnerability Classification” below and got assigned the CVE ID CVE-2021-41057. Successful exploitation of this vulnerability could allow an attacker to crash the CodeMeter Runtime Server (i.e., CodeMeter.exe), which could cause a denial-of-service condition for the affected Siemens product.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PSS(R)CAPE: CAPE 14 installations installed from material dated earlier than 2021-10-05	CAPE 14 installations installed from material dated 2021-10-05 or later are not affected, as they contain a fixed version of CodeMeter Runtime. If CAPE 14 was initially installed using earlier material, install WIBU Systems CodeMeter Runtime V7.30a manually to fix the issue: Download the package from https://www.psscrape.com/codemeter and install it the same way as documented for previous versions in the PSS CAPE 14 Installation Manual. Contact PSS(R)CAPE Support at psscrape.support.energy@siemens.com if you need assistance with patching affected systems.
PSS(R)E V34: All versions < V34.9.1	Update to V34.9.1 or later version Alternatively, install WIBU Systems CodeMeter Runtime V7.30a manually to fix the issue: Download the package from https://www.wibu.com/us/support/user/downloads-user-software.html and follow the installation instructions from WIBU Systems. Contact PSS(R) Support via the Customer Support Portal: https://siemens-pss.freshdesk.com/en/support/login , if you need assistance with patching affected systems. https://siemens-pss.com/

<p>PSS(R)E V35: All versions < V35.3.2</p>	<p>Update to V35.3.2 or later version Alternatively, install WIBU Systems CodeMeter Runtime V7.30a manually to fix the issue: Download the package from https://www.wibu.com/us/support/user/downloads-user-software.html and follow the installation instructions from WIBU Systems. Contact PSS(R) Support via the Customer Support Portal: https://siemens-pss.freshdesk.com/en/support/login, if you need assistance with patching affected systems. https://siemens-pss.com/</p>
<p>PSS(R)ODMS V12: All versions < V12.2.6.1</p>	<p>Update to V12.2.6.1 or later version Alternatively, install WIBU Systems CodeMeter Runtime V7.30a manually to fix the issue: Download the package from https://www.wibu.com/us/support/user/downloads-user-software.html and follow the installation instructions from WIBU Systems. Contact PSS(R) Support via the Customer Support Portal: https://siemens-pss.freshdesk.com/en/support/login, if you need assistance with patching affected systems. https://siemens-pss.com/</p>
<p>SICAM 230: All versions</p>	<p>Update SICAM 230 to V8.00 or later version. Then update CodeMeter Runtime to V7.30a: Download the package from: https://www.wibu.com/us/support/user/downloads-user-software.html. Install it on SICAM 230 systems according to the procedure documented in chapter 9.2 of the COPA-DATA Security Vulnerability Announcement 2021_2: https://www.copadata.com/fileadmin/user_upload/faq/files/CD_SVA_2021_2.pdf.</p>
<p>SIMATIC Information Server: All versions >= V2019 SP1</p>	<p>Harden the application server to prevent local access by untrusted personnel.</p>
<p>SIMATIC PCS neo: All versions</p>	<p>Harden the application server to prevent local access by untrusted personnel.</p>
<p>SIMATIC Process Historian (incl. Process Historian OPC UA Server): All versions >= V2019</p>	<p>Harden the application server to prevent local access by untrusted personnel.</p>
<p>SIMATIC WinCC OA V3.17: All versions</p>	<p>Limit local access to the WinCC OA server by hardening measures according to the security guideline.</p>
<p>SIMATIC WinCC OA V3.18: All versions</p>	<p>Limit local access to the WinCC OA server by hardening measures according to the security guideline.</p>

<p>SIMIT Simulation Platform: All versions >= V10.0</p>	<p>Install WIBU Systems CodeMeter Runtime V7.30a manually to fix the issue: Download the package from https://www.wibu.com/us/support/user/downloads-user-software.html and follow the installation instructions from WIBU Systems.</p>
--	---

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the [General Security Recommendations](#).

Product specific mitigations can be found in the section [Affected Products and Solution](#).

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

PSS(R)E is a power system simulation and analysis tool for power transmission operations and planning. It allows users to perform a wide variety of analysis functions, including power flow, dynamics, short circuit, contingency analysis, optimal power flow, voltage stability, transient stability simulation, and much more.

PSS(R)ODMS is a transmission network modeling and analysis tool that is designed to bridge the gap between multiple utility domains - including operations and planning.

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).

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

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-2021-41057

CodeMeter Runtime improperly controls file access permissions when running on Windows.

If local attackers with basic user capabilities manage to set up a link to a special system file used with CmDongles, they could overwrite essential files in the system and thereby crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

ADDITIONAL INFORMATION

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

- WIBU Systems Security Advisory WIBU-210910-01: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210910-01.pdf

- 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 (2021-11-09): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.