

## SSA-240541: WIBU Systems CodeMeter Heap Buffer Overflow Vulnerability in Industrial Products

Publication Date: 2023-09-12  
Last Update: 2024-05-14  
Current Version: V1.3  
CVSS v3.1 Base Score: 9.0

### SUMMARY

WIBU Systems published information about a heap buffer overflow vulnerability and associated fix releases of CodeMeter Runtime, a product provided by WIBU Systems and used in several Siemens industrial products for license management.

The vulnerability is described in the section 'Vulnerability Classification' below and got assigned the CVE ID CVE-2023-3935. Successful exploitation of this vulnerability could allow

- an unauthenticated remote attacker to execute code on vulnerable products, where CodeMeter Runtime (i.e., CodeMeter.exe) is configured as a server, or
- an authenticated local attacker to gain root/admin privileges on vulnerable products, where CodeMeter Runtime is configured as a client.

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

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PSS(R)CAPE V14: All versions < V14.2023-08-23 affected by <a href="#">all CVEs</a>	CAPE V14 installations installed from material dated 2023-08-23 or later are not affected, as they contain a fixed version of CodeMeter Runtime. For installations of CAPE V14 using material earlier than 2023-08-23: Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a>
PSS(R)CAPE V15: All versions < V15.0.22 affected by <a href="#">all CVEs</a>	Update to V15.0.22 or later version For affected versions: Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a>

<p>PSS(R)E V34: All versions &lt; V34.9.6 affected by <a href="#">all CVEs</a></p>	<p>Update to V34.9.6 or later version For affected versions: Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>PSS(R)E V35: All versions &lt; V35.6.1 affected by <a href="#">all CVEs</a></p>	<p>Update to V35.6.1 or later version For affected versions: Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>PSS(R)ODMS V13.0: All versions affected by <a href="#">all CVEs</a></p>	<p>Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>PSS(R)ODMS V13.1: All versions &lt; V13.1.12.1 affected by <a href="#">all CVEs</a></p>	<p>Update to V13.1.12.1 or later version For affected versions: Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from <a href="https://www.wibu.com/support/user/user-software.html">https://www.wibu.com/support/user/user-software.html</a> and follow the installation instructions from WIBU Systems. See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SIMATIC PCS neo V3: All versions affected by <a href="#">all CVEs</a></p>	<p>Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SIMATIC PCS neo V4.0: All versions affected by <a href="#">all CVEs</a></p>	<p>Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SIMATIC WinCC OA V3.17: All versions &lt; V3.17 P030 affected by <a href="#">all CVEs</a></p>	<p>Update to V3.17 P030 or later version <a href="https://www.winccoa.com/downloads/category/versions-patches.html">https://www.winccoa.com/downloads/category/versions-patches.html</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>

<p>SIMATIC WinCC OA V3.18: All versions &lt; V3.18 P021 affected by <a href="#">all CVEs</a></p>	<p>Update to V3.18 P021 or later version <a href="https://www.winccoa.com/downloads/category/versions-patches.html">https://www.winccoa.com/downloads/category/versions-patches.html</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SIMATIC WinCC OA V3.19: All versions &lt; V3.19 P006 affected by <a href="#">all CVEs</a></p>	<p>Update to V3.19 P006 or later version <a href="https://www.winccoa.com/downloads/category/versions-patches.html">https://www.winccoa.com/downloads/category/versions-patches.html</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SIMIT Simulation Platform: All versions &gt;= V10.0 &lt; V11.2 affected by <a href="#">all CVEs</a></p>	<p>Update to V11.2 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109954445/">https://support.industry.siemens.com/cs/ww/en/view/109954445/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SINEC INS: All versions &lt; V1.0 SP2 Update 2 affected by <a href="#">all CVEs</a></p>	<p>Update to V1.0 SP2 Update 2 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109825710/">https://support.industry.siemens.com/cs/ww/en/view/109825710/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>SINEMA Remote Connect: All versions affected by <a href="#">all CVEs</a></p>	<p>Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a></p>

## **WORKAROUNDS AND MITIGATIONS**

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

- If CodeMeter Runtime is configured as server: Limit remote access to systems where the CodeMeter Runtime network server is running
- If CodeMeter Runtime is configured as client only in the affected product: Ensure that only trusted persons have access to the system and avoid the configuration of additional local accounts

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

## **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.

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 CIM based network model management tool with network analysis capabilities for planning and operational planning targeting transmission utilities.

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

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 Simulation 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 DESCRIPTION**

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### **Vulnerability CVE-2023-3935**

In CodeMeter Runtime versions up to 7.60b, there is a heap buffer overflow vulnerability which can potentially lead to a remote code execution. Currently, no PoC is known to us. To exploit the heap overflow, additional protection mechanisms need to be broken. Remote access is only possible if CodeMeter is configured as a server. If CodeMeter is not configured as a server, the adversary would need to log in to the machine where the CodeMeter Runtime is running or trick the user into sending a malicious request to CodeMeter. This might result in an escalation of privilege. (WIBU-230704-01)

CVSS v3.1 Base Score	9.0
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-122: Heap-based Buffer Overflow

## **ADDITIONAL INFORMATION**

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

- WIBU Systems Security Advisory WIBU-230704-01: [https://cdn.wibu.com/fileadmin/wibu\\_downloads/security\\_advisories/Advisory\\_WIBU-230704-01.pdf](https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-230704-01.pdf)

The attack vector and impact depends on the configuration of CodeMeter Runtime (i.e., CodeMeter.exe) on a vulnerable product:

- If CodeMeter Runtime is configured as a server: an unauthenticated remote attacker could execute code on the system
- If CodeMeter Runtime is configured as a client: an authenticated local attacker could gain root/admin privileges on the system.

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 (2023-09-12): Publication Date  
V1.1 (2023-10-10): Added fix for PSS(R)E V35, SIMATIC WinCC OA V3.17 and SIMATIC WinCC OA V3.18; no fix planned for SIMATIC PCS neo V4.0  
V1.2 (2023-12-12): Added fix for SINEC INS  
V1.3 (2024-05-14): Added fix for SIMIT Simulation Platform

## **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](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.