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

Publication Date: 2023-09-12
Last Update: 2023-12-12
Current Version: V1.2
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	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 https://www.wibu.com/support/user/user-software.html and follow the installation instructions from WIBU Systems. See further recommendations from section Workarounds and Mitigations
PSS(R)CAPE V15: All versions < V15.0.22	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 https://www.wibu.com/support/user/user-software.html and follow the installation instructions from WIBU Systems. See further recommendations from section Workarounds and Mitigations

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

SIMATIC WinCC OA V3.18: All versions < V3.18 P021	Update to V3.18 P021 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.19: All versions < V3.19 P006	Update to V3.19 P006 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMIT Simulation Platform: All versions	Install WIBU Systems CodeMeter Runtime V7.60c or later version manually to fix the issue: Download the package from https://www.wibu.com/support/user/user-software.html and follow the installation instructions from WIBU Systems. Ensure that only trusted persons have access to the system and avoid the configuration of additional local accounts See further recommendations from section Workarounds and Mitigations
SINEC INS: All versions < V1.0 SP2 Update 2	Update to V1.0 SP2 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109825710/ See further recommendations from section Workarounds and Mitigations
SINEMA Remote Connect: All versions	Currently no fix is planned 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:

- 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
- If CodeMeter Runtime is configured as server: Limit remote access to systems where the CodeMeter Runtime network server is running

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 Simluation 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 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-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	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
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

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

TERMS OF USE