SSA-625850: Multiple WIBU Systems CodeMeter Vulnerabilities Affecting the Desigo CC Product Family

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.1

SUMMARY

Versions V5.0 through V7 of the Desigo CC product family (Desigo CC, Desigo CC Compact, Desigo CC Connect, Cerberus DMS) are affected by multiple vulnerabilities in the underlying third-party component WIBU Systems CodeMeter Runtime. Successful exploitation of these vulnerabilities could allow remote attackers to execute arbitrary code on the Desigo CC server, or create a denial of service condition. While all verison lines V5.0, V5.1 and V6 are affected by all listed vulnerabilities, V7 is only affected by CVE-2023-3935.

Siemens has released a patch to update the CodeMeter Runtime component and recommends to apply the patch on affected systems.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo CC product family V5.0: All versions	Install the patch (available at https://support.industry.siemens.com/cs/ww/en/view/109825787/), which can be applied to all released versions
Desigo CC product family V5.1: All versions	Install the patch (available at https://support.industry.siemens.com/cs/ww/en/view/109825787/), which can be applied to all released versions
Desigo CC product family V6: All versions	Install the patch (available at https://support.industry.siemens.com/cs/ww/en/view/109825787/), which can be applied to all released versions
Desigo CC product family V7: All versions affected by CVE-2023-3935	Install the patch (available at https://support.industry.siemens.com/cs/ww/en/view/109825787/), which can be applied to all released versions

WORKAROUNDS AND MITIGATIONS

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 affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Desigo CC product family consists of Desigo CC (an integrated building management platform for managing high-performing buildings), Desigo CC Compact (a tailored solution for small and medium-sized buildings), Desigo CC Connect (a software gateway based on the Desigo CC platform), and Cerberus DMS (a danger management station that helps users manage fire safety and security events).

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-2021-20093

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

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-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 vulnerabilities in CodeMeter Runtime refer to:

- WIBU Systems Security Advisory WIBU-210423-01: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-01.pdf
- WIBU Systems Security Advisory WIBU-210423-02: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-02.pdf
- WIBU Systems Security Advisory WIBU-230704-01: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-230704-01.pdf

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 (2023-11-14): Publication Date

TERMS OF USE