Product Security Advisory: WIBU-103401

Sharing rules

TLP:CLEAR
For the TLP version see: https://www.first.org/tlp/

Vulnerability Title

Vulnerabilities in CodeMeter Runtime If Configured as Server

Affected Products

Affected Products	Fixed Products
CodeMeter Runtime 9.x versions < 9.10 CodeMeter Runtime 8.x versions < 8.41a CodeMeter Runtime 7.x versions CodeMeter Runtime 6.x versions	CodeMeter Runtime 9.x versions >= 9.10 CodeMeter Runtime 8.x versions >= 8.41a

Vulnerability Details

Highest CVSSv3.1 Base Score	8.6
CVSSv3.1 Vector(s)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
Highest Severity	High

Requirements

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default. To verify the setting, check the profiling value `IsNetworkServer`:

- `IsNetworkServer=1` — configured as a server (affected).
- `IsNetworkServer=0` — not configured as a server.

Vulnerabilities

Improper Access Control in Local-Only Configuration Commands (CVE-0000-0001)

CVE-ID pending

A CVE-ID has been requested and is expected to be assigned by the end of August 2026. This advisory will be updated once the CVE-ID becomes available.

Description

If CodeMeter Runtime is configured as a server, the configuration command handler does not enforce network-origin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in `Server.ini`. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.

CWE: CWE-284:Improper Access Control

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime 9.x versions < 9.10	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
CodeMeter Runtime 8.x versions < 8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
CodeMeter Runtime 7.x versions	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
CodeMeter Runtime 6.x versions	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6

Fixed

- CodeMeter Runtime 9.x versions >= 9.10
- CodeMeter Runtime 8.x versions >= 8.41a

Remediations

Mitigation (2026-07-20T12:00:00.000Z)

If you enabled the network server functionality at some point but no longer need it, disable it:

If you are using CodeMeter 9.00 or newer, you can use `cmu --disable-network-server`

If you are using older versions of CodeMeter, do the following:

- On Windows, open the Registry Editor and navigate to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion\`, then change the value of `IsNetworkServer` from 1 to 0. Restart CodeMeter.
- On Linux and Mac, first stop CodeMeter, then edit the file under `/etc/wibu/CodeMeter/Server.ini`. Under `[General]`, change the value `IsNetworkServer` from 1 to 0. Then start CodeMeter again.

For products:

- CodeMeter Runtime 9.x versions < 9.10
- CodeMeter Runtime 8.x versions < 8.41a
- CodeMeter Runtime 7.x versions
- CodeMeter Runtime 6.x versions

Acknowledgments

- Andrew Teylu of Vector Informatik GmbH

Format String Vulnerability in Logger (CVE-0000-0002)

CVE-ID pending

A CVE-ID has been requested and is expected to be assigned by the end of August 2026. This advisory will be updated once the CVE-ID becomes available.

Description

The logger does not sanitize input strings in certain cases, allowing an attacker to inject `printf`-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using `cmu --set-proxy` to set the proxy value, and remotely when combined with CVE-0000-0001 by setting `General.ProxyServer` and then triggering this vulnerability.

CWE: CWE-134:Use of Externally-Controlled Format String

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime 9.x versions < 9.10	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
CodeMeter Runtime 8.x versions < 8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
CodeMeter Runtime 7.x versions	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2

Fixed

- CodeMeter Runtime 9.x versions >= 9.10
- CodeMeter Runtime 8.x versions >= 8.41a

Remediations

Mitigation (2026-07-20T12:00:00.000Z)

See remediation steps under CVE-0000-0001. Mitigation date: 2026-07-20.

For products:

- CodeMeter Runtime 9.x versions < 9.10
- CodeMeter Runtime 8.x versions < 8.41a
- CodeMeter Runtime 7.x versions

Acknowledgments

- Andrew Teylu of Vector Informatik GmbH

Missing Sanity Checks for Buffer Lengths (CVE-0000-0003)

CVE-ID pending

A CVE-ID has been requested and is expected to be assigned by the end of August 2026. This advisory will be updated once the CVE-ID becomes available.

Description

If configured as a server, CodeMeter Runtime accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.

CWE: CWE-130:Improper Handling of Length Parameter Inconsistency

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime 9.x versions < 9.10	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
CodeMeter Runtime 8.x versions < 8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

- CodeMeter Runtime 9.x versions >= 9.10
- CodeMeter Runtime 8.x versions >= 8.41a

Remediations

Mitigation (2026-07-20T12:00:00.000Z)

See remediation steps under CVE-0000-0001. Mitigation date: 2026-07-20.

For products:

- CodeMeter Runtime 9.x versions < 9.10
- CodeMeter Runtime 8.x versions < 8.41a

Acknowledgments

- Andrew Teylu of Vector Informatik GmbH

Improper Authentication of Session Handles (CVE-0000-0004)

CVE-ID pending

A CVE-ID has been requested and is expected to be assigned by the end of August 2026. This advisory will be updated once the CVE-ID becomes available.

Description

If configured as a server, CodeMeter Runtime issues handles per connection and relies on a cryptographically weak SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.

CWE: CWE-639:Authorization Bypass Through User-Controlled Key

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime 9.x versions < 9.10	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
CodeMeter Runtime 8.x versions < 8.41a	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7

CodeMeter Runtime 7.x versions	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
CodeMeter Runtime 6.x versions	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7

Fixed

- CodeMeter Runtime 9.x versions >= 9.10
- CodeMeter Runtime 8.x versions >= 8.41a

Remediations

Mitigation (2026-07-20T12:00:00.000Z)

See remediation steps under CVE-0000-0001. Mitigation date: 2026-07-20.

For products:

- CodeMeter Runtime 9.x versions < 9.10
- CodeMeter Runtime 8.x versions < 8.41a
- CodeMeter Runtime 7.x versions
- CodeMeter Runtime 6.x versions

Acknowledgments

- Andrew Teylu of Vector Informatik GmbH

WIBU-SYSTEMS AG

WIBU-SYSTEMS CERT
Zimmerstrasse 5
D-76137 Karlsruhe

Namespace: https://wibu.com

cert@wibu.com

Publishing Details

Publisher	WIBU-SYSTEMS AG
Webseite	https://www.wibu.com
Security Advisories	https://www.wibu.com/support/security-advisories.html

Document Details

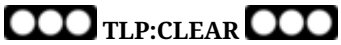
Document Name	WIBU-103401
Document version	1.1.0
Initial release date	2026-07-20T12:00:00.000Z
Current release date	2026-08-25T09:00:00.000Z
Language	en-US
Status	final
Also referred to	
Document category	csaf_security_advisory

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	2026-07-20T12:00:00.000Z	Initial Version
1.1.0	2026-08-25T09:00:00.000Z	First public version

Disclaimer

Sharing rules



For the TLP version see: https://www.first.org/tlp/