



NCSC-2026-0333

Kwetsbaarheden verholpen in CodeMeter Runtime van Wibu-Systems

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-08-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Wibu-Systems heeft meerdere kwetsbaarheden verholpen in CodeMeter Runtime.

Duiding

De kwetsbaarheden bevinden zich in verschillende onderdelen van CodeMeter Runtime, met name in versies voor 8.41a en 9.10. Een lokale aanvaller kan misbruik maken van onjuiste verificatie van NTFS reparse points bij het aanmaken van tijdelijke bestanden door cmu.exe, wat kan leiden tot het verwijderen van willekeurige systeembestanden met System-privileges en daarmee lokale privilege-escalatie.

Daarnaast bevat de configuratie command handler een fout waardoor netwerkrestricties niet correct worden afgedwongen, wat een aanvaller op afstand in staat stelt om ongeautoriseerde toegang te verkrijgen tot gevoelige configuratiegegevens en controle over de WebAdmin interface. Verder is er een input sanitization probleem in de logger module, waardoor format specifiers kunnen worden geïnjecteerd, wat kan leiden tot crashes en mogelijk informatielekken, zowel lokaal als op afstand, vooral in combinatie met CVE-2026-81573. Ook ontbreekt er correcte bounds checking op de data length in opcode 0x5e requests, wat een segmentation fault kan veroorzaken en de stabiliteit van de servercomponent kan beïnvloeden. Ten slotte wordt een zwakke SID gebruikt voor authenticatie, waardoor brute-force aanvallen mogelijk zijn om toegang te krijgen tot sessiehandles en daarmee tot licentie-informatie van andere sessies.

Oplossingen

Wibu-Systems heeft updates uitgebracht om deze kwetsbaarheden in CodeMeter Runtime te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.wibu.com/de/support/security-advisories/wibu-103081.html>
- <https://www.wibu.com/de/support/security-advisories/wibu-103401.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-81572	7.8 HIGH
➤ CVE-2026-81573	8.6 HIGH
➤ CVE-2026-81574	8.2 HIGH

> CVE-2026-81575	7.5 HIGH
> CVE-2026-81576	7.7 HIGH

CWE's

CWE	Beschrijving
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-125	Out-of-bounds Read
> CWE-130	Improper Handling of Length Parameter Inconsistency
> CWE-134	Use of Externally-Controlled Format String
> CWE-377	Insecure Temporary File
> CWE-639	Authorization Bypass Through User-Controlled Key

Getroffen producten

Wibu Systems
CodeMeter Runtime

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.