SECURITY ADVISORY

SPR-2609082, Ausgabe 1

8. September 2026

Sprecher Automation GmbH
Franckstraße 51, 4020 Linz / Österreich
Tel. +43 732 6908-0
Fax +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

Inhaltsverzeichnis

Wibu Systems-103401: Vulnerabilities in CodeMeter Runtime If Configured as Server

1. Zusammenfassung

Sprecher Automation wurde von WIBU-Systems über mehrere Schwachstellen in der WIBU-Systems CodeMeter Runtime informiert.

Die CodeMeter Runtime ist nur dann von den unten aufgeführten Schwachstellen betroffen, wenn sie als Server konfiguriert ist. Dies ist nicht die Standardeinstellung.
So überprüfen Sie die Einstellung:

- Öffnen Sie das CodeMeter Control Center, starten Sie WebAdmin und wechseln Sie zum Menü „Konfiguration/Server/Serverzugriff“. Überprüfen Sie das Optionsfeld „Netzwerkserver“
  - Aktiviert — als Server konfiguriert (betroffen).
  - Deaktiviert — nicht als Server konfiguriert.
- oder überprüfen Sie den Profilwert „IsNetworkServer“ im Registrierungseditor unter „Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion“:
  - IsNetworkServer=1 – als Server konfiguriert (betroffen).
  - IsNetworkServer=0 – nicht als Server konfiguriert.

1.1. Schwachstellen

Improper Access Control in Local-Only Configuration Commands (CVE-2026-81573)
Wenn CodeMeter Runtime als Server konfiguriert ist, erzwingt der "command handler" für die Konfiguration keine Einschränkungen hinsichtlich der Netzwerkherkunft. Befehle, die eigentlich nur für lokale Clients oder Clients im selben Netzwerk bestimmt sind, können daher von beliebigen Remote-Peers ausgeführt werden. Ein Angreifer kann potenziell sensible Konfigurationsdaten auslesen und ausgewählte Werte in der Datei „Server.ini“ überschreiben. Dazu gehört auch der Hash der Anmeldedaten für den CodeMeter WebAdmin, was eine Übernahme des WebAdmin ermöglicht.
CWE-284: Improper Access Control

Format String Vulnerability in Logger (CVE-2026-81574)
Der Logger bereinigt Eingabezeichenfolgen in bestimmten Fällen nicht, wodurch ein Angreifer Formatbezeichner im „printf“-Stil einschleusen kann. Dies kann genutzt werden, um CodeMeter zuverlässig zum Absturz zu bringen und sensible Informationen wie Prozessspeicher und Stack-Canaries offenzulegen. Der Angriff funktioniert lokal, beispielsweise durch Verwendung von `cmu --set-proxy` zum Festlegen des Proxy-Werts, sowie aus der Ferne in Kombination mit CVE-2026-81573, indem `General.ProxyServer` gesetzt und anschließend diese Schwachstelle ausgelöst wird.
CWE-134: Use of Externally-Controlled Format String

Missing Sanity Checks for Buffer Lengths (CVE-2026-81575)
Wenn CodeMeter Runtime als Server konfiguriert ist, akzeptiert es Anfragen mit dem Opcode 0x5e, die die Datenlänge und die Daten selbst enthalten. Eine fehlende Bereichsprüfung des Werts für die Datenlänge kann zu Lesezugriffen außerhalb des zulässigen Bereichs führen, was einen Segmentierungsfehler verursacht, der letztendlich zum Absturz von CodeMeter Runtime führt.
CWE-130: Improper Handling of Length Parameter Inconsistency

Improper Authentication of Session Handles (CVE-2026-81576)
Wenn CodeMeter Runtime als Server konfiguriert ist, vergibt es pro Verbindung Handles und nutzt eine kryptografisch schwache SID als einziges Authentifizierungsmittel. Ein Angreifer kann die SID per Brute-Force-Angriff knacken, die Handle-Nummer einer anderen Sitzung ermitteln und die zu einem anderen Handle gehörenden Lizenzinformationen auslesen.
CWE-639: Authorization Bypass Through User-Controlled Key

2. Betroffene Produkte und Versionen

SPRECON-V460 Versionen mit CodeMeter Runtime Versionen 6.x oder 7.x oder 8.x-Versionen < 8.41a oder 9.x-Versionen < 9.10.

3. Workarounds und Mitigationen

Improper Access Control in Local-Only Configuration Commands (CVE-2026-81573)
Aktualisieren der CodeMeter Runtime 8.x auf Version 8.41a oder höher.
Aktualisieren der CodeMeter Runtime 9.x auf Version 9.10 oder höher.

Workaround
Wenn Sie die Netzwerkserver-Funktionalität irgendwann aktiviert haben, diese aber nicht mehr benötigen, deaktivieren Sie sie:
Wenn Sie CodeMeter 9.00 oder neuer verwenden, können Sie den Befehl „cmu --disable-network-server“ verwenden.
Wenn Sie ältere Versionen von CodeMeter verwenden, gehen Sie wie folgt vor:

- Öffnen Sie das CodeMeter Control Center, starten Sie WebAdmin und wechseln Sie zum Menü „Konfiguration/Server/Serverzugriff“. Setzen Sie das Optionsfeld „Netzwerkserver“ auf „Deaktivieren“
- Oder
    - Öffnen Sie unter Windows den Registrierungseditor und navigieren Sie zu „Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion“. Ändern Sie dort den Wert von „IsNetworkServer“ von 1 auf 0. Starten Sie CodeMeter neu.
    - Unter Linux und Mac beenden Sie zunächst CodeMeter und bearbeiten Sie dann die Datei unter /etc/wibu/CodeMeter/Server.ini. Ändern Sie unter [General] den Wert von „IsNetworkServer“ von 1 auf 0. Starten Sie anschließend CodeMeter erneut.

Format String Vulnerability in Logger (CVE-2026-81574)
Siehe Workarounds & Mitigations CVE-2026-81573

Missing Sanity Checks for Buffer Lengths (CVE-2026-81575)
Siehe Workarounds & Mitigations CVE-2026-81573

Improper Authentication of Session Handles (CVE-2026-81576)
Siehe Workarounds & Mitigations CVE-2026-81573

4. Schwachstellen-Klassifizierung

CVE ID: **2026-81573**
CVSS 3.1 Score: 8.6
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L

CVE ID: **2026-81574**
CVSS 3.1 Score: 8.2
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVE ID: **2026-81575**
CVSS 3.1 Score: 7.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID: **2026-81576**
CVSS 3.1 Score: 7.7
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Das CVE®-Programm identifiziert, definiert und katalogisiert öffentlich bekannt gemachte Sicherheitslücken im Bereich der Cybersicherheit. Die Schwachstellen werden von Organisationen aus der ganzen Welt, die eine Partnerschaft mit dem CVE®-Programm eingegangen sind, entdeckt, zugewiesen und veröffentlicht. (Copyright © The MITRE Corporation https://www.cve.org/Legal/TermsOfUse)

CVSS ist ein offener Bewertungsrahmen, mit dem die Merkmale und der Schweregrad von Software-Schwachstellen angegeben werden können, wobei dies kein Maß für das Risiko ist. Dieser Standard ist auf der Website https://www.first.org/cvss/ dokumentiert.

5. Allgemeine Sicherheitsempfehlungen

Sprecher Automation empfiehlt die Einhaltung üblicher Sicherheitsempfehlungen allgemeiner und branchenspezifischer Standards und Normen wie z. B.:

- den lokalen physischen Zugang nur auf autorisierte Personen zu beschränken
- das Betriebssystem und die Software auf dem neuesten Stand zu halten

- Verwendung von Anwendungs-Whitelisting, um die Ausführung von Anwendungen auf die für den Betrieb des Systems erforderlichen Anwendungen zu beschränken
- das Testen von aktualisierten Versionen in einer Testumgebung, um den normalen Betrieb des Systems gemäß der projektspezifischen Konfiguration und Hardwareumgebung zu überprüfen, bevor das Update in einer Produktionsumgebung installiert wird
- dass ein Notfallplan vorhanden ist, um die Installation der Aktualisierung rückgängig zu machen, falls nach der Installation des Updates unerwartete Probleme in der Produktionsumgebung auftreten

6. Sprecher Automation PSIRT

Sprecher Automation hat ein **Product Security and Incident Response Team (PSIRT)**, um Risiken zu reduzieren, Cybersicherheit in den Produkten zu erhöhen und um IT Security-Zwischenfälle aufzulösen. Haben Sie oder Ihr Unternehmen eine Cybersicherheits-Schwachstelle in Produkten von Sprecher Automation gefunden, kontaktieren Sie uns bitte an der Funktionsadresse security@sprecher-automation.com. (Sollten Sie ein S/MIME-Zertifikat für verschlüsselte Kommunikation benötigen, können Sie ein E-Mail mit dem Betreff „Zertifikatsrequest“ an diese Adresse schicken.)

7. Dokumentenverlauf

2026-09-08 Veröffentlichungsdatum