SECURITY ADVISORY

SPR-2609081, 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

CVE-2026-81572: Wibu Systems-103081: Local Privilege Escalation in CodeMeter Runtime on Windows

1. Zusammenfassung

Sprecher Automation wurde von WIBU-Systems über eine Schwachstelle in der WIBU-Systems CodeMeter Runtime informiert.

Davon betroffen ist das CodeMeter Universal Support Tool (cmu.exe), das zur Verwaltung und Pflege von CodeMeter-Lizenzen und CmContainern verwendet wird.
„cmu.exe --create-io --file C:“ erstellt eine vorhersehbare temporäre Datei unter C:\CM-Stick. Die Verzeichnis- und Dateipfade werden vor der Durchführung von Dateioperationen nicht ordnungsgemäß auf NTFS-Reparse-Punkte wie Verknüpfungen oder symbolische Links überprüft. Ein lokaler Angreifer kann eine Verknüpfung zur temporären Datei erstellen, die auf einen beliebigen Systempfad verweist. Da die CodeMeter-Runtime mit Systemrechten ausgeführt wird, könnte dies dazu führen, dass beliebige Dateien mit Systemrechten gelöscht werden und möglicherweise eine lokale Rechteausweitung ermöglicht wird.

CWE-59: Improper Link Resolution Before File Access
https://cwe.mitre.org/data/definitions/59.html

2. Betroffene Produkte und Versionen

SPRECON-V460 Versionen mit CodeMeter Runtime 8.x-Versionen 8.40 - 8.41 oder 9.x-Versionen < 9.10.

3. Workarounds und Mitigationen

Aktualisieren der CodeMeter Runtime 8.x auf Version 8.41a oder höher.
Aktualisieren der CodeMeter Runtime 9.x auf Version 9.10 oder höher.

4. Schwachstellen-Klassifizierung

CVE ID: **2026-81572**

CVSS 3.1 Score: 7.8
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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