SECURITY ADVISORY

SPR-2506171, Ausgabe 1

17. Juni 2025

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-2025-47809: Privilege Escalation through CodeMeter Installer on Windows

1. Zusammenfassung

Der CodeMeter-Installer unter Windows weist einen Fehler auf, der unter bestimmten Umständen eine Rechteausweitung für ein Konto ohne Administratorrechte ermöglicht: Nach der Installation auf einem Konto ohne Administratorrechte mit UAC unter Verwendung des integrierten Administratorkontos startet CodeMeter das CodeMeter Control Center mit Systemrechten.

Sprecher Automation setzt für SPRECON-V460 Systeme eine Security-Grundhärtung voraus. Vor der Installation einer Software ist die Grundhärtung aufzuheben. Nach erfolgter Installation einer Software ist die Grundhärtung wieder zu Aktivieren. Basierend darauf wurde die folgende Schwachstellen-Klassifizierung vorgenommen.

2. Betroffene Produkte und Versionen

SPRECON-V460 bis einschließlich Version 14 mit installierter CodeMeter Runtime < 8.30a.

3. Workarounds und Mitigationen

SPRECON-V460 Systeme sind **nicht betroffen** und erfordern **keine Abhilfemaßnahmen**, wenn nach der Installation von CodeMeter eine der folgenden Aktionen durchgeführt wurde:

1. Das System wurde neu gestartet.
2. Der Benutzer hat sich abgemeldet.
3. Das CodeMeter Control Center wurde manuell geschlossen oder neu gestartet.

Darüber hinaus sind SPRECON-V460 Systeme in den folgenden Fällen **nicht betroffen**:

1. Das Benutzerkonto gehört zur **Administratorengruppe**.
2. CodeMeter Runtime wurde mit dem Parameter PROP_CMCC=„none“ oder PROP_CMCC=„auto“ installiert, da beide Optionen verhindern, dass das CodeMeter Control Center nach der Installation automatisch gestartet wird.

Abhilfemaßnahmen: Installation CodeMeter Runtime >= 8.30a.

4. Schwachstellen-Klassifizierung

CVSS 4.0 Score: 5.4
CVSS Vektor: AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA: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. In diesem Dokument wird die CVSS Version 4.x verwendet. 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

2025-06-17 Veröffentlichungsdatum