# SECURITY ADVISORY

SPR-2511041, Ausgabe 1

4. November 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-2025-41741: Potenzielle Schwachstelle durch statisches Schlüsselmaterial im Backupsystem

## 1. Zusammenfassung

Eine interne Sicherheitsprüfung hat ergeben, dass die SSM (Sprecher Storage Manager) Backup-Funktion statisches Schlüsselmaterial für die Ver- und Entschlüsselung von Sicherungsdateien verwendet. Diese Konfiguration stellt eine potenzielle Schwachstelle dar. Ein Angreifer, der sich Zugriff auf dieses Schlüsselmaterial verschafft, könnte theoretisch:

**Daten kompromittieren:** Gespeicherte Backups entschlüsseln, um sensible Systeminformationen oder Prozessdaten zu extrahieren.

**Integrität der Backups verletzen:** Werden Backups manipuliert und in das System zurückgespielt, könnte nicht autorisierter oder schädlicher Code zur Ausführung gebracht werden.

## 2. Betroffene Produkte und Versionen

Betroffen sind SPRECON-E-C/-E-P/-E-T3 mit Firmwareversionen kleiner 9.0

## 3. Workarounds und Mitigationen

Die Ausnutzung der beschriebenen Schwachstelle setzt einen **unbefugten physischen Zugriff** auf die Systemkomponenten voraus. Der Schutz von Anlagen vor unberechtigtem Zutritt ist daher eine essenzielle und effektive Schutzmaßnahme.

Wir empfehlen, die folgenden Schritte in Betracht zu ziehen und zu bewerten:

- **Grundlegende Sicherheitsmaßnahme:** Physischen Zugriffsschutz überprüfen
  Stellen Sie sicher, dass alle relevanten Systemkomponenten in einer überwachten und kontrollierten Umgebung (z.B. verschlossene Schaltschränke, zugangsgesicherte Räume) betrieben werden, um unautorisierten physischen Zugriff zu unterbinden.
- **Sofortmaßnahme zur Mitigation:** Temporäre Deaktivierung der SSM Backup-Funktion
  Als unmittelbare Maßnahme zur Risikominimierung empfehlen wir die temporäre Deaktivierung der SSM Backup-Funktion, falls diese nicht zwingend für den operativen Betrieb erforderlich ist.
  **Wichtiger Hinweis:** Bitte evaluieren Sie vor der Deaktivierung die Auswirkungen auf Ihre Backup- und Wiederherstellungsprozesse und stellen Sie sicher, dass eine alternative Backup-Strategie vorhanden ist.
- **Ergänzende Maßnahme:** Überwachung der Systemkonfiguration
  Wir raten zu einer kontinuierlichen Überwachung der Systemkonfiguration. Dadurch können unautorisierte Änderungen, wie beispielsweise eine unerwartete Reaktivierung der betroffenen Funktion, zeitnah erkannt werden.

- **Behebung:** Update und Verwendung eines kundenspezifischen/eigenen Schlüsselmaterials
  Update auf Firmwareversion 9.0 oder höher.

# 4. Schwachstellen-Klassifizierung

**CVE ID:** **CVE-2025-41741**

CVSS 3.1 Score: 6.7
CVSS Vektor: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 4.0 Score: 8.7
CVSS Vektor: CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA: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. Danksagungen

Sprecher Automation dankt Sec-Consult Security Labs für die Identifizierung und verantwortungsvolle Meldung dieser Schwachstelle.

# 7. 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.)

# 8. Dokumentenverlauf

| | |
|---|---|
| 2025-11-04 | Veröffentlichungsdatum |