SECURITY ADVISORY

SPR-2511043, 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

1. Zusammenfassung 2
2. Betroffene Produkte und Versionen 2
3. Workarounds und Mitigationen 2
3.1. Firmwareupdate 2
3.2. Kompensierende Maßnahmen 2
4. Schwachstellen-Klassifizierung 3
5. Allgemeine Sicherheitsempfehlungen 3
6. Danksagungen 3
7. Sprecher Automation PSIRT 3
8. Dokumentenverlauf 4

CVE-2025-41743: Angreifbare Verschlüsselung der Update Dateien

1. Zusammenfassung

Im Rahmen einer Sicherheitsprüfung wurde festgestellt, dass die Verschlüsselung von Firmware-Images unzureichend ist. Ein Angreifer, der im Besitz einer solchen Firmware-Datei ist, könnte diese Schwachstelle ausnutzen, um das Image zu entpacken und zu analysieren. Dies könnte dem Angreifer detaillierte Informationen über die Systemarchitektur und interne Funktionsweisen offenlegen.

Wichtige Einschränkung:
Die Integrität des Systems ist durch diese Schwachstelle **nicht direkt gefährdet**. Der robuste Signaturprüfungsmechanismus der Firmware bleibt intakt und wirksam. Ein **Angreifer ist nicht in der Lage**, eine modifizierte Firmware zu erstellen, die vom System als gültig akzeptiert wird. Eine unautorisierte Codeausführung oder Manipulation des laufenden Systems ist auf diesem Weg nicht möglich.

2. Betroffene Produkte und Versionen

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

3. Workarounds und Mitigationen

3.1. Firmwareupdate

Ein Update auf Firmware-Version 9.0 oder höher ist möglich – dies behebt die Schwachstelle vollständig. Die Implementierung der Verschlüsselung wurde in der Firmware-Version 9.0 vollständig überarbeitet und durch einen stärkeren Mechanismus ersetzt.

3.2. Kompensierende Maßnahmen

- **Sichere Ablage von Firmware-Dateien:** Behandeln Sie Firmware-Dateien als sensible Informationen. Speichern Sie diese ausschließlich auf Systemen mit strenger Zugriffskontrolle (z.B. gesicherte Fileserver, Engineering-Stationen). Stellen Sie durch Berechtigungskonzepte sicher, dass nur autorisiertes Personal Zugriff auf diese Dateien hat.
- **Verwendung vertrauenswürdiger Quellen**: Beziehen Sie Firmware-Dateien ausschließlich über unsere offiziellen und gesicherten Kanäle. Vermeiden Sie die Verwendung von Firmware-Images aus unbekannten oder ungesicherten Quellen (z.B. ungesicherte USB-Sticks, öffentliche Netzwerklaufwerke).

4. Schwachstellen-Klassifizierung

CVE ID: **CVE-2025-41743**

CVSS 3.1 Score: 3.3
CVSS Vektor: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 4.0 Score: 4.0
CVSS Vektor: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/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. 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