SECURITY ADVISORY

SPR-2511044, 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-2025-41744: Statisches Default Schlüsselmaterial bei TLS Verbindungen

1. Zusammenfassung

SPRECON-E Geräte werden mit einem Default-Zertifikat für den integrierten Webserver sowie andere Dienste mit TLS-Unterstützung ausgeliefert. Dieses Zertifikat ist auf allen Geräten ident und dient ausschließlich der initialen Inbetriebnahme. Wird dieses Zertifikat nicht durch ein individuelles/kundeneigenes, einzigartiges Zertifikat ersetzt, entsteht ein das Potential für Sicherheitsrisiko. **Diese Maßnahme wird im Leitfaden „SPRECON Grundhärtung“ empfohlen.**

1.1. Details

Risiko und Angriffsszenario: Ein Angreifer mit Zugriff auf ein beliebiges SPRECON-E Gerät (oder die Firmware-Datei) könnte das Default-Zertifikat inklusive des privaten Schlüssels extrahieren. Mit diesem Schlüsselmaterial wäre der Angreifer in der Lage, einen Man-in-the-Middle (MITM) Angriff gegen jedes andere SPRECON-E Gerät durchzuführen, das noch das Default-Zertifikat verwendet.
Bei einem erfolgreichen MITM-Angriff kann der Angreifer den gesamten Netzwerkverkehr zwischen dem Benutzer und dem Webserver des SPRECON-E Gerätes abhören, entschlüsseln und gegebenenfalls manipulieren. Dies könnte zur Kompromittierung von Anmeldedaten, zur Offenlegung sensibler Konfigurationsdaten oder zur Manipulation der an den Benutzer angezeigten Informationen führen.

2. Betroffene Produkte und Versionen

Betroffen sind SPRECON-E-C/-E-P/-E-T3

3. Workarounds und Mitigationen

Wie im Leitfaden „SPRECON Grundhärtung“ beschrieben, ist der Austausch des Default-Zertifikats ein obligatorischer Schritt im Rahmen der sicheren Konfiguration und Inbetriebnahme eines SPRECON-E Gerätes. Wir empfehlen Ihnen, die Einhaltung dieser Sicherheitsmaßnahme zu überprüfen.

3.1. Unmittelbare Maßnahme: Ersetzen des Default-Zertifikats

Wir empfehlen allen Betreibern, umgehend zu überprüfen, ob auf ihren SPRECON-E Geräten noch das werkseitige Default-Zertifikat im Einsatz ist.

- Falls ja, sollte dieses dringend durch ein individuelles/kundeneigenes, einzigartiges Zertifikat ersetzt werden.
- Detaillierte Anweisungen finden Sie im Leitfaden „SPRECON Grundhärtung“ bzw. im Benutzerhandbuch „SPRECON-E Designer“.

3.2. Organisatorische Maßnahme: Audit der Gerätekonfiguration

Integrieren Sie die Überprüfung des Webserver-Zertifikats in Ihre regelmäßigen Sicherheits-Audits und Konfigurations-Reviews, um sicherzustellen, dass alle Geräte korrekt konfiguriert sind.

4. Schwachstellen-Klassifizierung

CVE ID: **CVE-2025-41744**

CVSS 3.1 Score: 8.8
CVSS Vektor: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 4.0 Score: 8.7
CVSS Vektor: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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