SECURITY ADVISORY

SPR-2511042, 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-2025-41742: Kritische Schwachstelle durch Verwendung statischer kryptografischer Schlüssel in Systemkomponenten

1. Zusammenfassung

Eine Sicherheitsanalyse hat ergeben, dass an mehreren Stellen statische, nicht-einzigartige kryptografische Schlüssel verwendet werden. Dies führt zu zwei potenziellen Risiken:

Mögliche Fehlidentifizierung von Anlagen:
Ein statischer Mechanismus zur Anlagen-Identifizierung im Wartungsprozess kann umgangen werden. Dies betrifft nicht die benutzerspezifische Authentifizierung, diese erfolgt separat. Das Hauptrisiko besteht darin, dass ein bereits authentifizierter Benutzer Wartungsarbeiten an der falschen Anlage durchführt.

Kompromittierung von Projektdateien:
Die Verschlüsselung von Projekt-, Konfigurations- und Wartungsdateien basiert auf statischem Schlüsselmaterial, was die Vertraulichkeit und Integrität dieser Daten gefährdet.

1.1. Details

1.1.1. Mangelhafte Anlagen-Identifizierung im Wartungsprozess

Der Mechanismus, der eine Anlage im Wartungsprozess eindeutig identifizieren soll, kann mit einem statischen, systemweit identen Wert umgangen werden.

Risiko: Ein autorisierter Techniker, könnte sich im Zuge von Wartungsarbeiten versehentlich oder absichtlich mit einer falschen Anlage verbinden. Das Aktivieren einer Konfiguration oder die Installation eines Firmware-Updates auf einer dafür nicht vorgesehenen Anlage kann zu Betriebsstörungen führen. Die Gefahr liegt in der operativen Fehlhandlung eines legitimierten Nutzers.

1.1.2. Statische Schlüssel für Projekt- und Konfigurationsdateien

Projekt-, Konfigurations- und Wartungsdateien werden mit einem statischen, systemweiten Schlüssel verschlüsselt.

Risiko: Ein Angreifer mit Zugriff auf diese Dateien könnte das Schlüsselmaterial extrahieren, um sensible Informationen wie z. B. Systemarchitektur oder Prozesslogik einzusehen. Des Weiteren könnten die Dateien manipuliert und wieder verschlüsselt werden. Die Verwendung manipulierter Dateien im Engineering-System oder in der Anlage, könnte zu unerwünschtem Systemverhalten führen.

2. Betroffene Produkte und Versionen

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

3. Workarounds und Mitigationen

3.1. Kontinuierliche Überwachung der Systemintegrität

Um unautorisierte Änderungen an Projekt- und Parametrierdateien zeitnah zu erkennen, sollten Konfigurationsdateien regelmäßig überprüft werden.

- **Nutzung von SNMP-Funktionen:** Das System bietet die Möglichkeit, über SNMP (Simple Network Management Protocol) Statusinformationen und Konfigurations-Checksummen auszulesen. Integrieren Sie diese Abfragen in Ihr zentrales Netzwerk-Monitoring-System (NMS). Richten Sie Alarme ein, die ausgelöst werden, wenn sich eine Checksumme unerwartet ändert. Dies dient als Frühwarnsystem für potenzielle Manipulationen.
- **Manuelle Integritätsprüfungen:** Führen Sie in regelmäßigen Abständen manuelle Vergleiche der Konfigurationsdateien mit einem bekannten, sicheren "Golden Image" (Referenz-Backup) durch.

3.2. Härtung der Zugriffskontrollen (Defense-in-Depth)

Ein mehrschichtiger Sicherheitsansatz ist die effektivste Methode, um unbefugten Zugriff zu verhindern, der die Voraussetzung für die Ausnutzung dieser Schwachstellen ist.

- **Physischer Schutz:** Stellen Sie sicher, dass alle Steuerungskomponenten, Engineering-Stationen und Netzwerkgeräte in zugangsgeschützten Bereichen (z.B. verschlossenen Schaltschränken, gesicherten Serverräumen) untergebracht sind, um unbefugten physischen Zugriff zu unterbinden.
- **Netzwerksegmentierung:** Betreiben Sie die Automatisierungssysteme in einem strikt segmentierten Netzwerk, das durch Firewalls vom Büro- und Internet-Netzwerk getrennt ist. Der Zugriff für Wartungsarbeiten sollte nur von dedizierten, gesicherten Management-Clients aus erlaubt sein.
- **Prinzip der geringsten Rechte (Least Privilege):** Vergeben Sie Benutzerrechte restriktiv. Jeder Benutzer sollte nur jene Berechtigungen erhalten, die für die Ausführung seiner spezifischen Aufgaben zwingend erforderlich sind. Dies minimiert das Schadenspotenzial, falls ein Benutzerkonto kompromittiert wird oder ein autorisierter Benutzer einen Fehler macht.

4. Schwachstellen-Klassifizierung

CVE ID: **CVE-2025-41742**

CVSS 3.1 Score: 9.6
CVSS Vektor: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

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