SECURITY ADVISORY

SPR-2407171, Ausgabe 1

17. Juli 2024

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-2024-6758: Protection Assignments Roles Escalation

1. Zusammenfassung

Mit Hilfe von speziell generierten HTTP(S)-Requests können Schutzzuweisungen mit reduzierten Rechten unabhängig von der Rollenzuweisung gespeichert werden.

Dies setzt voraus, dass ein Zugriff auf die Webschnittstelle konfiguriert wurde. Ein direktes Ausnutzen der Schwachstelle über die Weboberfläche ist nicht möglich.

2. Betroffene Produkte und Versionen

SPRECON-E, Firmwareversion < 8.71j

3. Workarounds und Mitigationen

Behebung über eine Aktualisierung auf die Firmwareversion >= 8.71j

Als Mitigationsmaßnahmen können eine oder mehrere der folgenden Maßnahmen durchgeführt werden:

- Deaktivierung des Gastzugriffs, Zugriff nur mit entsprechender Authentifizierung und Rollenzuweisung erlauben.
- Nach der Deaktivierung des Webservers ist eine Ausnutzung der Schwachstelle nicht mehr möglich.
- Schränken Sie mit Hilfe der Firewall den Zugriff auf http(s) ein und erlauben Sie nur den Zugriff von definierten Adressbereichen oder Adressen.

4. Schwachstellen-Klassifizierung

CVE-ID: CVE-2024-6758
CVSS 3.1 Score: 6.5
CVSS Vektor: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
Beschreibung: Protection Assignments Roles Escalation

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 3.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

2024-07-17 Veröffentlichungsdatum