SECURITY ADVISORY

SPR-2411261, Ausgabe 1

26. November 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-2024-3596: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS)

1. Zusammenfassung

Das RADIUS-Protokoll nach RFC 2865 ist anfällig für Fälschungsangriffe durch einen lokalen Angreifer, der jede gültige Antwort (Access-Accept, Access-Reject oder Access-Challenge) in eine beliebige andere Antwort umwandeln kann, indem er einen Angriff mit gewählter Präfix-Kollision gegen die MD5 Response Authenticator-Signatur durchführt.
Um die Schwachstelle auszunutzen, muss sich der Angreifer im aktiven Datenpfad befinden (Man-in-the-Middle-Angriff).

2. Betroffene Produkte und Versionen

SPRECON-E: Firmware-Versionen < 8.71k

SPRECON-T3: Firmware-Versionen < 8.71m

SPRECON-V460: Betroffen sind Projekte, welche das IIoT Identity Service mit RADIUS Authentifizierung in der Service Engine benutzen.

3. Workarounds und Mitigationen

SPRECON-E: Es sind keine Workarounds verfügbar. Ab Firmware Version 8.71k ist die Schwachstelle behoben.

SPRECON-T3: Es sind keine Workarounds verfügbar. Ab Firmware Version 8.71m ist die Schwachstelle behoben.

SPRECON-V460: Es sind keine Workarounds oder Mitigationen verfügbar.

4. Schwachstellen-Klassifizierung

CVE ID:	CVE-2024-3596
CVSS 3.1 Score:	8.1
CVSS Vektor:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Beschreibung:	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS)

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 3.1 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

2024-11-26 Veröffentlichungsdatum