SECURITY ADVISORY

SPR-2508251, Ausgabe 1

25. August 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

zenon/SPRECON-V460 Remote Transport Vulnerability

1. Zusammenfassung

Die Schwachstelle in der Service Engine kann nur dann ausgenutzt werden, wenn ein Benutzer eine bewusste Interaktion mit dem Remote Transport Service auf einem Engineering Studio Rechner anstößt. Mit dem Remote Transport Service werden die Engineering Studio Projektdaten auf einen Ziel-Rechner (Service Engine) übertragen.

Die Schwachstelle ermöglicht die Nutzung der Reboot OS-Funktionalität des Remote Transport Service ohne ordnungsgemäße Authentifizierung auf einem Ziel-Rechner, der Service Engine (Runtime). Die Reboot OS-Funktionalität fordert einen Neustart des Ziel-Rechners. Die Schwachstelle kann nicht aus der Ferne ausgenutzt werden, ohne zuvor Zugriff auf das Netzwerk zu erlangen, in dem sich der Ziel-Rechner befindet.

Zum Zeitpunkt der Erstellung dieses Dokuments gibt es keine Hinweise darauf, dass diese Schwachstelle aktiv ausgenutzt wird.

2. Betroffene Produkte und Versionen

Die Datei „zensyssrv.exe“, die in der Remote-Transport-Funktionalität in Engineering Studio verwendet wird, ist von dieser Schwachstelle betroffen. Die Auswirkung betrifft die verbundene Service Engine (Runtime), nicht das Engineering Studio.

Die Softwareplattform-Versionen 8.20, 10, 11, 12 und 14 sind von dieser Schwachstelle betroffen. Ein Patch ist für die genannten Versionen verfügbar.

Alle Versionen bis einschließlich Softwareplattform 8.10 sind betroffen. Für Softwareplattform-Versionen, die nicht im Support-Lebenszyklus für das Jahr 2025 enthalten sind, sind keine Patches geplant.

3. Workarounds und Mitigationen

- Beschränken Sie den Netzwerkzugriff auf Systeme, auf denen die Softwareplattform installiert ist. Stellen Sie sicher, dass der Zugriff auf ein System durch Zugriffskontrollen eingeschränkt ist, um das Risiko eines unbefugten Zugriffs zu minimieren.

- Bewerten Sie die Notwendigkeit der Remote-Transport-Funktionalität.
  Stellen Sie sicher, dass bei Nichtverwendung der Remote-Transport-Funktionalität die zensyssrv.exe (zenon System Service) gestoppt oder beendet wird. Die zensyssrv.exe kann auch nach autorisierter Nutzung gestoppt oder beendet werden, um diese Schwachstelle zu vermeiden.

Die Schwachstelle wurde für die Versionen 8.20, 10, 11, 12 und 14 behoben:

- Version 14 Build 350309 und höher
- Version 12 Build 352417 und höher
- Version 11 Build 383048 und höher
- Version 10 Build 348998 und höher
- Version 8.20 Build 381546 und höher

Die Plattform-Build-Setups können im Download-Bereich heruntergeladen werden (Benutzerregistrierung erforderlich).

4. Schwachstellen-Klassifizierung

CVSS 4.0 Score: 6.9 / Medium
CVSS Vektor: AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:H/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. In diesem Dokument wird die CVSS Version 4.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

2025-08-25 Veröffentlichungsdatum