31. Juli 2023

SPRECON-V460
SICHERHEITS-SCHWACHSTELLEN MITTEILUNG 2023-07 AUSGABE 1

IIoT-Dienste unter Windows (früher Service Grid), Service Engine unter Windows

PRODUKT MANAGEMENT SPRECON-V460

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

1. Historie

Datum	Ausgabe	Bemerkung
31.07.2023	1	Erstellt

2. Einführung

Sprecher Automation informiert über einen Bericht von Copa-Data, in dem eine Sicherheitslücke für SPRECON-V460 beschrieben wird.

Diese Schwachstellen betreffen Systeme, auf denen SPRECON-V460 installiert ist.

3. Betroffene Produkte

IIoT Services unter Windows (früher Service Grid) und die Service Engine unter Windows sind von diesen Schwachstellen betroffen.

4. Betroffene Versionen

Alle Service-Grid-Versionen bis einschließlich Version 11 sind von CVE-2023-3321 betroffen.

Alle Service Engine-Versionen sind von CVE-2023-3323 betroffen.

Die Service-Engine-Versionen 7.60 und höher sind von CVE-2023-3324 betroffen..

5. Details zur Schwachstelle

Ein Angreifer, der die Sicherheitslücke CVE-2023-3321 erfolgreich ausnutzt, kann den Data Hub dazu bringen, beliebigen Code in einem erhöhten Kontext zu laden und auszuführen. Dies setzt voraus, dass ein Angreifer Zugriff auf einen Windows-Rechner hat, auf dem die Service-Grid-Komponenten installiert sind, dass keine Anwendungs-Whitelisting- oder ähnliche Technologien verwendet werden, um die Ausführung von nicht vertrauenswürdigem Code zu verhindern. Ein Angreifer kann eine maßgeschneiderte Datei, die den auszuführenden Code enthält, auf dem Rechner platzieren und eine Konfigurationsdatei für die zu ladende Datei des Angreifers ändern.

Ein Angreifer, der die Sicherheitslücke CVE-2023-3323 erfolgreich ausnutzt, kann die Service Engine dazu veranlassen, Code auszuführen, der nicht für die Ausführung durch den Projektingenieur vorgesehen war. Dies setzt voraus, dass ein Angreifer Zugriff auf ein System mit dem Engineering Studio hat, auf dem die Service Engine gestartet ist, auf dem das Engineering Studio die Service Engine-Dateien nicht kompiliert oder überschreibt und die Service Engine-Dateien im Standardverzeichnis erzeugt werden.

Ein Angreifer, der die Sicherheitslücke CVE-2023-3324 erfolgreich ausnutzt, kann die Service-Engine dazu veranlassen, Dateiinhalte mit einer als unsicher erkannten Methode zu deserialisieren, was dazu führen kann, dass die Service-Engine in einen unbekannten Zustand gerät oder möglicherweise Code ausführt.

Dies setzt voraus, dass:

- ein Angreifer Zugang zu einem Rechner mit der Service Engine hat.
- das Projekt ein Bild enthält.

- das Bild ein WPF-Element enthält, das so konfiguriert ist, dass es eine vom 3D-Konfigurationswerkzeug erstellte .cdwpf-Datei verwendet.
- der Bildschirm entweder automatisch oder durch Interaktion des Benutzers geöffnet wird.
- die Service-Engine-Dateien in einem Verzeichnis gespeichert sind, auf das der Angreifer Schreibzugriff hat.
- der Angreifer eine bestimmte Datei so konstruieren kann, dass die von der .cdwpf verwendete Deserialisierungsmethode in einen ungültigen Zustand geraten kann.

5.1. CVE-2023-3321 Data Hub – unsichere Dateiberechtigungen

Es besteht eine Schwachstelle im Data Hub, bei der der Data Hub eine zusätzliche Konfigurationsdatei zum Laden von Plugins berücksichtigt, die in einem Verzeichnis gespeichert ist, auf das ein normaler Benutzer Schreibzugriff hat.

CVSS v3.1 Basiswert und Vektor:

Für diese Sicherheitslücke wurde eine CVSS-Basisbewertung von **7.0** berechnet.

Der entsprechende CVSS v3.1 Vektor:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C&version=3.1

5.2. CVE-2023-3323 Unsichere Dateiberechtigungen für das Standardverzeichnis der Service-Engine-Dateien

Es besteht eine Schwachstelle in den Dateiberechtigungen für das Standardverzeichnis, in dem das Engineering Studio anwendungsrelevante Service Engine-Dateien ablegt. Die Gruppe "Jeder" hat Schreibzugriff auf den Standardordner.

CVSS v3.1 Basiswert und Vektor:

Für diese Sicherheitslücke wurde eine CVSS-Basisbewertung von **5.9** berechnet.

Der entsprechende CVSS v3.1 Vektor:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:P/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C&version=3.1

5.3. CVE-2023-3324 Unsichere Deserialisierungsmethode

Das WPF-Element des 3D-Steuerelements in der Service-Engine verwendet eine Deserialisierungsmethode, die nicht mehr als sicher gilt.

CVSS v3.1 Basiswert und Vektor:

Für diese Sicherheitslücke wurde eine CVSS-Basisbewertung von **6.3** berechnet.

Der entsprechende CVSS v3.1 Vektor:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H/E:U/RL:U/RC:R&version=3.1

6. Maßnahmen

Es gibt Optionen und Empfehlungen zur Risikominderung, die das Risiko von Schwachstellen verringern. Die praktische Anwendung der Maßnahmenoptionen hängt vom Anwendungsfall und der Art der Nutzung der Technologie ab.

6.1. Maßnahmen für CVE-2023-3321

Auf Windows-Systemen, auf denen die IIoT Services (ehemals Service Grid)-Komponenten installiert sind, stellen Sie die Zugriffssteuerung in Windows ein, um den Schreibzugriff auf die Datei "mosquitto.conf" auf Administrator-Benutzer zu beschränken.
Auf Windows-Systemen, auf denen die IIoT Services (Service Grid) Komponenten nicht benötigt werden, sollten diese Komponenten entfernt werden.

6.1. Maßnahmen für CVE-2023-3323

Ändern Sie auf Windows-Systemen mit dem Engineering Studio und auf Systemen mit der Service Engine die Berechtigungen des Ordners "C:\Benutzer\Öffentlich\Öffentliche Dokumente\SPRECON-V460_Projects" und entfernen Sie die Gruppe "Jeder". Fügen Sie die Gruppe "Users" mit Lese- und Schreibberechtigung hinzu. Alternativ erstellen und definieren Sie eine (lokale) Gruppe für Engineering Studio-Ingenieure mit Lese- und Schreibrechten für den Ordner "SPRECON-V460_Projects" und weisen Sie dieser Gruppe Benutzer zu, die das Engineering Studio zum Erstellen/Kompilieren von Service Engine-Dateien verwenden dürfen.

Als weitere Möglichkeit können Sie den Arbeitsbereich und die Service-Engine-Dateien in einem anderen Ordner als dem Standardordner erstellen und die entsprechenden Berechtigungen für den alternativen Ordner entsprechend festlegen.

6.2. Maßnahmen für CVE-2023-3324

Im Folgenden wird beschrieben, wie Sie WPF-Elemente, die mit dem 3D Konfigurator Tool erstellt wurden, aus Projekten entfernen können.
Im Engineering Studio:

- Entfernen Sie die vom 3D Konfigurator Tool erstellten .cdwpf-Dateien aus dem Ordner Graphics in den Projekten.
- WPF-Elemente aus den Bildern in den Projekten entfernen.

Erstellen Sie Service-Engine-Dateien für die geänderten Projekte.
Auf dem System mit der Service Engine:

- Aktualisieren Sie die Service-Engine-Dateien.
- Entfernen Sie den Ordner "ThreeD" aus dem Ordner "Service Engine".

7. Update Verfügbarkeit

SPRECON-V460 12 (das erste Release der Version erscheint in Kürze) behebt CVE-2023-3321.
Die Konfigurationsdatei wird an einem anderen Ort installiert, an dem nur Administratorbenutzer Schreibrechte haben.

Für SPRECON-V460 11 sind aktualisierte MSI-Dateien für relevante Komponenten verfügbar, die die Schwachstelle auf dieselbe Weise wie in Version 12 beheben.
Für bestehende Installationen in SPRECON-V460 11 ist eine Deinstallation mit anschließender Installation der aktualisierten MSI-Dateien erforderlich.

SPRECON-V460 12 führt eine neue 3D-Integration ein, die das bestehende 3D-Konfigurationswerkzeug und das 3D-WPF-Element ersetzen soll, aber eine Änderung des Projekts erfordert. Die neue 3D-Integration ist nicht von CVE-2023-3321 betroffen.

8. Allgemeine Empfehlungen

Sprecher Automation empfiehlt,

- den lokalen physischen Zugang nur auf autorisierte Personen zu beschränken.
- Verwendung des SPRECON-V460 Engineering Studio auf einem separaten Engineering-System in einer geschützten Umgebung, auf das nur autorisierte Benutzer Zugriff haben und auf dem geeignete Sicherheitsmaßnahmen wie die Verwendung von Anwendungs-Whitelisting und Antiviren-Software vorhanden sind.
- die Installation der IIoT Services (früher bekannt als Service Grid) Komponenten auf einem dedizierten System. Alternativ können diese Komponenten auch in einer Docker-Umgebung auf einem Linux-Host ausgeführt werden.
- das Betriebssystem und die Software auf dem neuesten Stand zu halten.
- Verwendung von Anwendungs-Whitelisting, um die Ausführung von Anwendungen auf die Anwendungen zu beschränken, die für den Betrieb des Systems erforderlich sind.
- das Testen der aktualisierten Version der SPRECON-V460-Software 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.

9. Danksagung

Sprecher Automation bedankt sich bei Copa-Data für die Unterstützung bei der Identifizierung der Schwachstellen und beim Schutz unserer Partner und Kunden.