SECURITY ADVISORY SPRECON-V460 & SPRECON-TOOLS

SPR_SPRECON-V_2023-08, Ausgabe 2

8. September 2023

Updates gegenüber der vorherigen Ausgabe sind rot markiert

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 2023-3935: Heap buffer overflow in Wibu Systems CodeMeter Runtime can potentially lead to (remote) code execution

1. Zusammenfassung

Sprecher Automation wurde über eine Sicherheitslücke in der Wibu Systems CodeMeter User Runtime Software unterrichtet, wonach über einen Buffer Overflow eine Code Execution ermöglicht wird, welche je nach Installation potentiell über Netzwerk ausnutzbar ist. Die Schwachstelle weist einen CVSS 3.1 Score von 9.0 auf.

Die CodeMeter User Runtime Software wird von SPRECON-V460 für den Software-Lizenzschutz verwendet. Das Problem wurde von Wibu Systems behoben und eine neue Version 7.60c der CodeMeter User Runtime Software steht zur Verfügung, welche die Schwachstelle behebt. Auf bestehenden SPRECON-V460 Installationen kann diese Runtime ausgetauscht/aktualisiert werden ohne das V460 System aktualisieren / neu installieren zu müssen.

Darüber hinaus wird die CodeMeter User Runtime ebenfalls bei SPRECON-Tools für die Lizenzierung verwendet (SPRECON-E Service Programm, SPRECON-E Designer, SPRECON-E PLC Designer, SPRECON-E Display Editor), allerdings nur wenn mittels Wibu CodeMeter USB-Dongle lizenziert wird und hierfür das SPRECON Licensing Driver Package installiert wurde.

2. Betroffene Produkte und Versionen

Hinweis: Die CodeMeter User Runtime Software kann auch von Softwareprodukten anderer Hersteller verwendet werden. Es sollte also auf jeden Fall geprüft werden, ob diese Software installiert ist. CodeMeter User Runtime Software Versionen bis 7.60b sind betroffen und sollten aktualisiert werden.

2.1. SPRECON-V460

Die CodeMeter User Runtime Software wird zur Dongle- und Softlizenzierung von Engineering Studio/Editor, Service Engine/Runtime, Report Engine/Analyzer, Smart Server/Webserver, Logic Service/Logic Runtime, dem Logic Studio/Logic Workbench und IIoT Services/ServiceGrid verwendet. Die CodeMeter User Runtime Software ist Teil der Installation dieser Softwareprodukte, auch wenn keine Dongle Lizenz verwendet wird.

- SPRECON-E V460 Versionen ab 6.50 können prinzipiell betroffen sein. Die Versionen höher als 8.00 verwenden ausschließlich die CodeMeter User Runtime Software von Wibu Systems und sind von dieser Sicherheitslücke definitiv betroffen.
- Versionen bis einschließlich 8.00 verwenden möglicherweise die CodeMeter User Runtime Software von Wibu Systems und könnten von dieser Schwachstelle betroffen sein.
- Alle Reporting Engine/ Analyzer Versionen verwenden die CodeMeter User Runtime Software von Wibu Systems und sind von dieser Sicherheitslücke betroffen.

2.2. SPRECON-Tools

Die CodeMeter User Runtime wird ebenfalls bei SPRECON-Tools für die Dongle Lizenzierung verwendet (SPRECON-E Service Programm, SPRECON-E Designer, SPRECON-E PLC Designer, SPRECON-E Display Editor). Wird eines dieser Tools auf einen CodeMeter USB-Dongle lizenziert, so muss hierfür das SPRECON Licensing Driver Package installiert werden, welches wiederum die CodeMeter Runtime installiert. Alle SPRECON Licensing Driver Packages bis inkl. 1.13 SP1 sind von dieser Schwachstelle betroffen. Erst mit 1.13 SP2 liefert das Package die aktuelle CodeMeter Runtime 7.60c.

3. Workarounds und Mitigationen

Bei einer Standardinstallation von SPRECON-V460 und auch SPRECON Licensing Driver Package ist die CodeMeter Runtime nicht so konfiguriert, dass sie als CodeMeter Runtime Server fungiert. In diesem Fall existiert die Schwachstelle nur lokal am jeweiligen System, wodurch sich der CVSS Temporal Score auf 7.1 reduziert. Über die CodeMeter WebAdmin Oberfläche kann überprüft werden, ob es sich um eine lokale Installation oder einen Runtime Server handelt.

Wenn die CodeMeter Runtime so konfiguriert ist, dass sie als CodeMeter Runtime Server fungiert, werden CodeMeter Lizenzen für SPRECON-V460 Produkte über das Netzwerk bereitstellt, somit ergibt die Schwachstelle den CVSS Basis-Score 9.0 und ist über Netzwerk ausnutzbar.

Wibu Systems stellt mit dem Advisory WIBU-230704-01 zusätzliche Informationen zur Verfügung:
https://www.wibu.com/de/support/security-advisories.html

Sprecher Automation empfiehlt die CodeMeter User Runtime – sofern vorhanden - am System zu aktualisieren. Diese wird vom Hersteller in Version 7.60c bereitgestellt:
https://www.wibu.com/support/user/downloads-user-software.html

3.1. Workarounds

Die folgenden Maßnahmen werden empfohlen, um das Risiko zu verringern, bis die korrigierte Version installiert werden kann. Bitte beachten Sie, dass nicht alle Abhilfemaßnahmen für jede mögliche Produktkonfiguration gelten. Prüfen Sie daher, welche dieser Maßnahmen in Ihrem Fall relevant oder anwendbar sein könnten.

- Schränken Sie den unprivilegierten Zugriff auf Maschinen ein, auf denen die CodeMeter User Runtime Software ausgeführt wird, um eine lokale Ausnutzung der Schwachstelle zu verhindern.
- Konfigurieren Sie die Lizenzzugriffsrechte im CodeMeter WebAdmin für die CodeMeter User Runtime Software, und beschränken Sie den Zugriff auf die Rechner, die eine Lizenz von diesem CodeMeter Runtime Server benötigen.
- Aktivieren Sie HTTPS für den CodeMeter WebAdmin, um eine sichere Verbindung zur Konfigurationsoberfläche zu gewährleisten.

- Verweigern Sie den Fernlesezugriff auf den CodeMeter WebAdmin, wenn die Administration lokal durchgeführt werden kann
- Konfigurieren Sie die Authentifizierung für den Lese- und Schreibzugriff für den CodeMeter WebAdmin, um zu verhindern, dass unberechtigte Benutzer Änderungen durchführen können.

3.2. Updateprozedur

Für bestehende Installationen mit einer CodeMeter Lizenz ist es notwendig, die aktualisierte CodeMeter User Runtime Software für Windows von Wibu Systems herunterzuladen und diese Version auf den betroffenen Systemen zu installieren, um die Sicherheitslücke zu beheben.

Das Installationsprogramm der CodeMeter User Runtime Software für Windows ist in der Lage, eine bestehende Installation zu aktualisieren. Es ist nicht erforderlich, die bestehende CodeMeter User Runtime Software für Windows zu deinstallieren.

Schließen Sie alle Anwendungen während der Installation der aktualisierten CodeMeter User Runtime Software für Windows.

Führen Sie einen Neustart des Systems durch, um die Aktualisierung erfolgreich abzuschließen.

Wenn die CodeMeter Lizenz als lokale Lizenz verwendet wird (wahrscheinlichstes Szenario) und nicht als Netzwerklizenz verwendet wird, ist es nicht erforderlich, die CodeMeter Runtime als CodeMeter Runtime Server zu konfigurieren.

Die CodeMeter User Runtime Software ist mit aktuellen Windows-Versionen kompatibel.

4. Schwachstellen-Klassifizierung

CVE ID:	**2023-3935**
CVSS 3.1 Score:	9.0
CVSS Vektor:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Beschreibung:	Heap buffer overflow in CodeMeter Runtime can potentially lead to (remote) code execution.

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

2023-08-23:	Ausgabe 1	Veröffentlichungsdatum
2023-09-08:	Ausgabe 2	Ergänzung SPRECON-Tools