SECURITY ADVISORY

SPR-2407171, Issue 1

17 July 2024

Sprecher Automation GmbH
Franckstrasse 51, 4020 Linz / Austria
T: +43 732 6908-0
F: +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

Contents

Disclaimer: This document contains a general analysis and classification and is not tailored to the Customer's specific systems and configurations. The information and details are merely recommendations and therefore are to be applied by the Customer correspondingly to its own systems and configurations and implemented at its own discretion and under its own responsibility. No liability or guarantee for correctness or completeness is given.

CVE 2024-6758: Protection Assignments Roles Escalation

1. Summary

With the use of specially generated HTTP(S) requests, protection assignments with reduced rights can be saved independently of the role assignment.

This requires that access to the web interface has been configured. Direct exploitation of the vulnerability via the web interface is not possible.

2. Affected Products and Versions

SPRECON-E, Firmwareversion < 8.71j

3. Workarounds and Mitigations

Mitigation via an update to firmware version >= 8.71j

One or more of the following measures can be implemented as workaround measures:

- Disable guest access, allow access only with appropriate authentication and role assignment.
- Once the web server has been deactivated, it is no longer possible to exploit the vulnerability.
- Use the firewall to restrict access to http(s) and only allow access from defined address ranges or addresses.

4. Vulnerability Classification

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

The CVE® programme identifies, defines and catalogues publicly disclosed cyber security vulnerabilities. Vulnerabilities are discovered, assigned and published by organisations from around the world that have partnered with the CVE® programme. (Copyright © The MITRE Corporation https://www.cve.org/Legal/TermsOfUse)

CVSS is an open assessment framework that can be used to indicate the characteristics and severity of software vulnerabilities, whereby this is not a measure of risk. CVSS version 3.x is used in this document. This standard is documented on the website https://www.first.org/cvss/.

5. General Security Recommendations

Sprecher Automation recommends compliance with common safety recommendations of general and industry-specific standards and norms. E. g.:

- to restrict local physical access to authorised persons only
- keeping the operating system and software up to date
- using application whitelisting to restrict the execution of applications to those required for the operation of the system
- testing updated versions in a test environment to verify normal operation of the system according to the project-specific configuration and hardware environment before installing the update in a production environment
- that a disaster recovery plan is in place to reverse the installation of the update if unexpected problems occur in the production environment after the update has been installed

6. Sprecher Automation PSIRT

Sprecher Automation has a **Product Security and Incident Response Team (PSIRT)** to reduce risks, increase cyber security in products and resolve IT security incidents. If you or your company have found a cybersecurity vulnerability in Sprecher Automation products, please contact us at the functional address security@sprecher-automation.com. (If you need an S/MIME certificate for encrypted communication, you can send an email with the subject "Certificate Request" to this address).

7. Document History

2024-07-17	Publication date