SECURITY ADVISORY

SPR-2511043, Issue 1

4 November 2025

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

CVE-2025-41743: Vulnerable encryption of update files

1. Summary

During a security audit, it was discovered that the encryption of firmware images is insufficient. An attacker in possession of such a firmware file could exploit this vulnerability to unpack and analyze the image. This could reveal detailed information about the system architecture and internal workings to the attacker.

Important limitation:
The integrity of the system is **not directly compromised** by this vulnerability. The robust signature verification mechanism of the firmware remains intact and effective. An **attacker cannot** create modified firmware that will be accepted as valid by the system. Unauthorized code execution or manipulation of the running system is not possible in this way.

2. Affected Products and Versions

SPRECON-E-C/-E-P/-E-T3 with firmware versions lower than 9.0 are affected.

3. Workarounds and Mitigations

3.1. Firmware update

An update to firmware version 9.0 or higher is available – this completely resolves the vulnerability. The implementation of encryption has been completely revised in firmware version 9.0 and replaced with a stronger mechanism.

3.2. Compensatory measures

- **Secure storage of firmware files:** Treat firmware files as sensitive information. Store them exclusively on systems with strict access control (e.g., secure file servers, engineering stations). Use authorization concepts to ensure that only authorized personnel have access to these files.
- **Use trusted sources:** Obtain firmware files exclusively through our official and secure channels. Avoid using firmware images from unknown or unsecured sources (e.g., unsecured USB sticks, public network drives).

4. Vulnerability Classification

CVE ID: **CVE-2025-41743**

CVSS 3.1 Score: 3.3
CVSS Vektor: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 4.0 Score: 4.0
CVSS Vektor: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

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. 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. Acknowledgements

Sprecher Automation would like to thank Sec-Consult Security Labs for identifying and responsibly reporting this vulnerability.

7. 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).

8. Document History

2025-11-04 Publication date