SECURITY ADVISORY

SPR-2511041, 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-2025-41741: Potential vulnerability due to static key material in the backup system

1. Summary

An internal security audit has revealed that the SSM (Sprecher Storage Manager) backup function uses static key material for encrypting and decrypting backup files. This configuration represents a potential vulnerability. An attacker who gains access to this key material could theoretically:

Compromise data: Decrypt stored backups to extract sensitive system information or process data.

Violate the integrity of backups: If backups are manipulated and restored to the system, unauthorized or malicious code could be executed.

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

Exploiting the vulnerability described requires **unauthorized physical access** to the system components. Protecting systems from unauthorized access is therefore an essential and effective protective measure.

We recommend considering and evaluating the following steps:

- **Basic security measure:** Check physical access security.

Ensure that all relevant system components are operated in a monitored and controlled environment (e.g., locked control cabinets, access-secured rooms) to prevent unauthorized physical access.

- **Immediate mitigation measure:** Temporary deactivation of the SSM backup function

As an immediate risk mitigation measure, we recommend temporarily deactivating the SSM backup function if it is not absolutely necessary for operational purposes.
Important note: Before deactivating the function, please evaluate the impact on your backup and recovery processes and ensure that an alternative backup strategy is in place.

- F Monitoring of the system configuration

We recommend continuous monitoring of the system configuration. This allows unauthorized changes, such as unexpected reactivation of the affected function, to be detected promptly.

- **Resolving:** Update and use of client-specific/own key material

Update to firmware version 9.0 or higher.

4. Vulnerability Classification

CVE ID: **CVE-2025-41741**

CVSS 3.1 Score: 6.7
CVSS Vektor: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 4.0 Score: 8.7
CVSS Vektor: CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

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