SECURITY ADVISORY

SPR-2511044, 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-2025-41744: Static default key material for TLS connections

1. Summary

SPRECON-E devices are delivered with a default certificate for the integrated web server and other services with TLS support. This certificate is identical on all devices and is used exclusively for initial commissioning. If this certificate is not replaced by an individual/customer-specific, unique certificate, this creates a potential security risk. **This measure is recommended in the "SPRECON Basic Hardening" guide.**

1.1. Details

Risk and attack scenario: An attacker with access to any SPRECON-E device (or the firmware file) could extract the default certificate, including the private key. With this key material, the attacker would be able to carry out a man-in-the-middle (MITM) attack against any other SPRECON-E device that still uses the default certificate.
In the event of a successful MITM attack, the attacker could intercept, decrypt, and, if necessary, manipulate all network traffic between the user and the web server of the SPRECON-E device. This could lead to the compromise of login credentials, the disclosure of sensitive configuration data, or the manipulation of the information displayed to the user.

2. Affected Products and Versions

SPRECON-E-C/-E-P/-E-T3 are affected.

3. Workarounds and Mitigations

As described in the "SPRECON Basic Hardening" guide, replacing the default certificate is a mandatory step in the secure configuration and commissioning of a SPRECON-E device. We recommend that you verify compliance with this security measure.

3.1. Immediate action: Replacing the default certificate

We recommend that all operators immediately check whether the factory default certificate is still in use on their SPRECON-E devices.

- If so, it should be replaced urgently with an individual/customer-specific, unique certificate.
- Detailed instructions can be found in the "SPRECON Basic Hardening" guide or in the "SPRECON-E Designer" user manual.

3.2. Organizational measure: Audit of device configuration

Integrate the verification of the web server certificate into your regular security audits and configuration reviews to ensure that all devices are configured correctly.

4. Vulnerability Classification

CVE ID: **CVE-2025-41744**

CVSS 3.1 Score: 8.8
CVSS Vektor: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 4.0 Score: 8.7
CVSS Vektor: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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