SECURITY ADVISORY

SPR-2508251, Issue 1

25 August 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

zenon/SPRECON-V460 Remote Transport Vulnerability

1. Summary

The vulnerability in the Service Engine can only be exploited if a user initiates a deliberate interaction with the Remote Transport Service on an Engineering Studio computer. The Remote Transport Service is used to transfer Engineering Studio project data to a target computer (Service Engine).

The vulnerability allows the Reboot OS functionality of the Remote Transport Service to be used without proper authentication on a target computer, the Service Engine (Runtime). The Reboot OS functionality requires a restart of the target computer. The vulnerability cannot be exploited remotely without first gaining access to the network in which the target computer is located.

At the time of writing, there is no evidence that this vulnerability is being actively exploited.

2. Affected Products and Versions

The zensyssrv.exe, which is used in the Remote Transport functionality in the Engineering Studio is affected by this vulnerability. The impact is on connected Service Engine (Runtime), not on the Engineering Studio.

The Software Platform versions 8.20, 10, 11, 12 and 14 are affected by this vulnerability. A patch is available for the mentioned versions.

All versions prior to and including Software Platform 8.10 are affected. No patches are planned for Software Platform version not included in the Support Life Cycle for the year 2025.

3. Workarounds and Mitigations

- Restrict network access to systems with the Software Platform installed.
  Ensure that access to a system is restricted by implementing access controls to minimize the risk of unauthorized access.

- Assess the necessity of the Remote Transport functionality.
  Ensure that if the Remote Transport functionality is not used, the zensyssrv.exe (System Service) is stopped or terminated. The zensyssrv.exe can also be stopped or terminated after authorized use to prevent this vulnerability.

The vulnerability has been resolved for versions 8.20, 10, 11, 12, and 14:

- Version 14 build 350309 and higher
- Version 12 build 352417 and higher

- Version 11 build 383048 and higher
- Version 10 build 348998 and higher
- Version 8.20 build 381546 and higher

Platform Build Setups can be downloaded from the download area (requires user registration)

4. Vulnerability Classification

CVSS 4.0 Score: 6.9 / Medium
CVSS Vektor: AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:H/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. CVSS version 4.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

2025-08-25 Publication date