TLP:WHITE

# VDE-2025-019: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers

| | |
|---|---|
| Publisher: Phoenix Contact GmbH & Co. KG | Document category: csaf_security_advisory |
| Initial release date: Tue Jul 08 12:00:00 CEST 2025 | Engine: 2.5.26 |
| Current release date: Tue Jul 08 12:00:00 CEST 2025 | Build Date: Tue Jul 01 09:54:50 CEST 2025 |
| Current version: 1 | Status: FINAL |
| CVSSv3.1 Base Score: 9.8 | Severity: Critical |
| Original language: | Language: en-GB |
| Also referred to: VDE-2025-019, PCSA-2025-00002 | |

## Summary

Multiple vulnerabilities in the firmware of CHARX SEC-3xxx charging controllers have been discovered.

## General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

## Impact

The vulnerabilities can lead to a total loss of confidentiality, integrity and availability of the devices.

## Mitigation

Affected charging controllers are designed and developed for the use in closed industrial networks. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

## Remediation

Phoenix Contact strongly recommends to upgrade to firmware version 1.7.3 which fixes these vulnerabilities.

## Product Description

CHARX EVSE charging controller

## Product groups

**Affected products.**

- FW <1.7.3 installed on CHARX SEC-3150
- FW <1.7.3 installed on CHARX SEC-3100
- FW <1.7.3 installed on CHARX SEC-3050
- FW <1.7.3 installed on CHARX SEC-3000

**Fixed products.**

- FW 1.7.3 installed on CHARX SEC-3150
- FW 1.7.3 installed on CHARX SEC-3100
- FW 1.7.3 installed on CHARX SEC-3050
- FW 1.7.3 installed on CHARX SEC-3000

# Vulnerabilities

## CVE-2025-25268

### Summary

An unauthenticated adjacent attacker can modify configuration by sending specific requests to an API-endpoint resulting in read and write access due to missing authentication.

**CWE:** CWE-306: Missing Authentication for Critical Function

## Product status

### Known affected

| Product | CVSS-Vector | CVSS Base Score |
|---|---|---|
| FW <1.7.3 installed on CHARX SEC-3150 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3100 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3050 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3000 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |

### Fixed

| Product |
|---|
| FW 1.7.3 installed on CHARX SEC-3150 |
| FW 1.7.3 installed on CHARX SEC-3100 |
| FW 1.7.3 installed on CHARX SEC-3050 |
| FW 1.7.3 installed on CHARX SEC-3000 |

## Acknowledgments

- HT3 Labs for reporting.

## CVE-2025-25269

### Summary

An unauthenticated local attacker can inject a command that is subsequently executed as root, leading to a privilege escalation.

**CWE:** CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

## Product status

### Known affected

| Product | CVSS-Vector | CVSS Base Score |
|---|---|---|
| FW <1.7.3 installed on CHARX SEC-3150 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.4 |
| FW <1.7.3 installed on CHARX SEC-3100 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.4 |
| FW <1.7.3 installed on CHARX SEC-3050 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.4 |
| FW <1.7.3 installed on CHARX SEC-3000 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.4 |

### Fixed

| Product |
|---|
| FW 1.7.3 installed on CHARX SEC-3150 |
| FW 1.7.3 installed on CHARX SEC-3100 |
| FW 1.7.3 installed on CHARX SEC-3050 |
| FW 1.7.3 installed on CHARX SEC-3000 |

## Acknowledgments

- HT3 Labs for reporting.

# CVE-2025-25270

### Summary

An unauthenticated remote attacker can alter the device configuration in a way to get remote code execution as root with specific configurations.

**CWE:** CWE-913: Improper Control of Dynamically-Managed Code Resources

## Product status

### Known affected

| Product | CVSS-Vector | CVSS Base Score |
|---|---|---|
| FW <1.7.3 installed on CHARX SEC-3150 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 |
| FW <1.7.3 installed on CHARX SEC-3100 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 |
| FW <1.7.3 installed on CHARX SEC-3050 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 |
| FW <1.7.3 installed on CHARX SEC-3000 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 |

### Fixed

| Product |
| --- |
| FW 1.7.3 installed on CHARX SEC-3150 |
| FW 1.7.3 installed on CHARX SEC-3100 |
| FW 1.7.3 installed on CHARX SEC-3050 |
| FW 1.7.3 installed on CHARX SEC-3000 |

## Acknowledgments

- Tobias Scharnowski, Felix Buchmann, Kristian Covic from fuzzware.io for reporting.

# CVE-2025-25271

### Summary

An unauthenticated adjacent attacker is able to configure a new OCPP backend, due to insecure defaults for the configuration interface.

**CWE:** CWE-1188: Initialization of a Resource with an Insecure Default

## Product status

### Known affected

| Product | CVSS-Vector | CVSS Base Score |
| --- | --- | --- |
| FW <1.7.3 installed on CHARX SEC-3150 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3100 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3050 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |
| FW <1.7.3 installed on CHARX SEC-3000 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 8.8 |

### Fixed

| Product |
| --- |
| FW 1.7.3 installed on CHARX SEC-3150 |
| FW 1.7.3 installed on CHARX SEC-3100 |
| FW 1.7.3 installed on CHARX SEC-3050 |
| FW 1.7.3 installed on CHARX SEC-3000 |

## Acknowledgments

- The Synacktiv team for reporting.

# Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for coordination. (see: https://certvde.com/en/)
- ZDI for coordination.

# Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

# References

- PCSA-2025-00002 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2025-019: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-019
- VDE-2025-019: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-019.json
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

# Revision history

| Version | Date of the revision | Summary of the revision |
|---|---|---|
| 1 | Tue Jul 08 12:00:00 CEST 2025 | Initial Revision |

# Sharing rules

**TLP:WHITE**
For the TLP version see https://www.first.org/tlp/