

# VDE-2024-070: Phoenix Contact: Security Advisory for CHARX-SEC3xxx Charge controllers

|  |   |
|--|---|
| Publisher: Phoenix Contact GmbH & Co. KG           | Document category: csaf_security_advisory |
| Initial release date: Tue Jan 14 12:00:00 CET 2025 | Engine: 2.5.15                            |
| Current release date: Tue Jan 14 11:00:00 CET 2025 | Build Date: Tue Jan 14 11:00:00 CET 2025  |
| Current version: 1                                 | Status: FINAL                             |
| CVSSv3.1 Base Score: 8.8                           | Severity: <a href="#">high</a>            |
| Original language:                                 | Language: en-GB                           |
| Also referred to: VDE-2024-070, PCSA-2024/00022    |   |

## Summary

Improper file permission handling allows an authenticated low privileged user to gain root access.

## General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: [Application Note Security](#)

## Impact

This vulnerability allows the authenticated user "user-app" to gain root rights (privilege escalation).

## Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to General Recommendation.

## Remediation

Phoenix Contact strongly recommends upgrading affected charge controllers to firmware version 1.7.0 or higher which fixes this vulnerability.

## Product Description

CHARX control modular AC are charging controllers for mode 3 electric vehicle charging.

## Product groups

### Affected Products.

- Firmware < 1.7.0 installed on CHARX SEC-3000
- Firmware < 1.7.0 installed on CHARX SEC-3050
- Firmware < 1.7.0 installed on CHARX SEC-3100
- Firmware < 1.7.0 installed on CHARX SEC-3150

### Fixed Products.

- Firmware 1.7.0 installed on CHARX SEC-3000
- Firmware 1.7.0 installed on CHARX SEC-3050
- Firmware 1.7.0 installed on CHARX SEC-3100
- Firmware 1.7.0 installed on CHARX SEC-3150

## Vulnerabilities

### CVE-2024-11497

#### Summary

An authenticated attacker can use this vulnerability to perform a privilege escalation to gain root access.

**CWE:** CWE-732: Incorrect Permission Assignment for Critical Resource

**Release date:** Tue Jan 14 11:00:00 CET 2025

#### Product status

#### Known affected

| Product   | CVSS-Vector                                  | CVSS Base Score |
|---|--|-----------------|
| Firmware < 1.7.0 installed on CHARX SEC-3000<br>Order number: 1139022 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | 8.8             |
| Firmware < 1.7.0 installed on CHARX SEC-3050<br>Order number: 1139018 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | 8.8             |
| Firmware < 1.7.0 installed on CHARX SEC-3100<br>Order number: 1139012 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | 8.8             |
| Firmware < 1.7.0 installed on CHARX SEC-3150<br>Order number: 1138965 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | 8.8             |

#### Fixed

##### Product

Firmware 1.7.0 installed on CHARX SEC-3000  
Order number: 1139022 ([Download](#))

Firmware 1.7.0 installed on CHARX SEC-3050  
Order number: 1139018 ([Download](#))

Firmware 1.7.0 installed on CHARX SEC-3100  
Order number: 1139012 ([Download](#))

Firmware 1.7.0 installed on CHARX SEC-3150  
Order number: 1138965 ([Download](#))

# Acknowledgments

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

- CERTVDE for coordination (see: <https://certvde.com>)
- Tien Phan, Richard Jaletzki for reporting

# Phoenix Contact GmbH & Co. KG

Namespace: <https://phoenixcontact.com/psirt>

[psirt@phoenixcontact.com](mailto:psirt@phoenixcontact.com)

# References

- PCSA-2024/00022: (EXTERNAL): <https://phoenixcontact.com/psirt>
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): <https://certvde.com/de/advisories/vendor/phoenixcontact/>
- Phoenix Contact application note (EXTERNAL): [https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913\\_en\\_03.pdf](https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf)
- VDE-2024-070: Phoenix Contact: Security Advisory for CHARX-SEC3xxx Charge controllers - HTML (SELF): <https://certvde.com/en/advisories/VDE-2024-070/>
- VDE-2024-070: Phoenix Contact: Security Advisory for CHARX-SEC3xxx Charge controllers - CSAF (SELF): <https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2024/vde-2024-070.json>

# Revision history

| Version | Date of the revision         | Summary of the revision |
|---------|------------------------------|-------------------------|
| 1       | Tue Jan 14 12:00:00 CET 2025 | initial revision        |

# Sharing rules

**TLP:WHITE**

For the TLP version see <https://www.first.org/ttp/>