TLP:WHITE

VDE-2025-014: 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: 2.5.27
Current release date: Tue Jul 08 12:00:00 CEST 2025	Build Date: Tue Jul 01 09:46:11 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 8.2	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2025-014, PCSA-2025-00001	

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 vulnerabilities CVE-2025-24005 and CVE-2025-24006. The vulnerabilities CVE-2025-24002, CVE-2025-24003 and CVE-2025-24004 affect the Eichrecht functionality in FW <=1.6.5 and in the meantime there is no vendor fix planned for these issues.

Product Description

CHARX SEC 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
- FW <=1.6.5 installed on CHARX SEC-3150
- FW <=1.6.5 installed on CHARX SEC-3100
- FW <=1.6.5 installed on CHARX SEC-3050
- FW <=1.6.5 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-2025-24002

Summary

An unauthenticated remote attacker can use MQTT messages to crash a service on charging stations complying with German Calibration Law, resulting in a temporary denial-of-service for these stations until they got restarted by the watchdog.

CWE: CWE-20: Improper Input Validation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
FW <=1.6.5 installed on CHARX SEC-3150	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
FW <=1.6.5 installed on CHARX SEC-3100	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
FW <=1.6.5 installed on CHARX SEC-3050	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
FW <=1.6.5 installed on CHARX SEC-3000	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Acknowledgments

- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

CVE-2025-24003

Summary

An unauthenticated remote attacker can use MQTT messages to trigger out-of-bounds writes in charging stations complying with German Calibration Law, resulting in a loss of integrity for only EichrechtAgents and potential denial-of-service for these stations.

CWE: CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
FW <=1.6.5 installed on CHARX SEC-3150	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.2
FW <=1.6.5 installed on CHARX SEC-3100	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.2
FW <=1.6.5 installed on CHARX SEC-3050	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.2
FW <=1.6.5 installed on CHARX SEC-3000	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	8.2

Acknowledgments

- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

CVE-2025-24004

Summary

A physical attacker with access to the device display via USB-C can send a message to the device which triggers an unsecure copy to a buffer resulting in loss of integrity and a temporary denial-of-service for the stations until they got restarted by the watchdog.

CWE: CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
FW <=1.6.5 installed on CHARX SEC-3150	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L	5.2
FW <=1.6.5 installed on CHARX SEC-3100	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L	5.2
FW <=1.6.5 installed on CHARX SEC-3050	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L	5.2
FW <=1.6.5 installed on CHARX SEC-3000	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L	5.2

Acknowledgments

- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

CVE-2025-24005

Summary

A local attacker with a local user account can leverage a vulnerable script via SSH to escalate privileges to root due to improper input validation.

CWE: CWE-20: Improper Input Validation

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:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3100	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3050	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3000	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

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

- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

CVE-2025-24006

Summary

A low privileged local attacker can leverage insecure permissions via SSH on the affected devices to escalate privileges to root.

CWE: CWE-269: Improper Privilege Management

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:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3100	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3050	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
FW <1.7.3 installed on CHARX SEC-3000	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

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

- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

Acknowledgments

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

- CERTVDE for coordination. (see: https://certvde.com/en/)
- Jesson Soto Ventura, Matthew Waddell from ivision for reporting.

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025-00001 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2025-014: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-014
- VDE-2025-014: Phoenix Contact: Security Advisory for CHARX SEC-3xxx charging controllers - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-014.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/