Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

Phoenix Contact GmbH & Co. KG · 32825 Blomberg

[2024/00002]

# Security Advisory for CHARX SEC-3xxx charge controllers

Publication Date: 2024-03-12
Last Update: 2024-03-12
Current Version: V1.0

## Advisory Title

Multiple vulnerabilities have been discovered in the Firmware of CHARX SEC-3xxx charge controllers. These vulnerabilities were discovered as part of a PWN2OWN competition initiated by Trend Micro Zero Day Initiative (ZDI).

## Advisory ID

CVE-2024-25994, CVE-2024-25995, CVE-2024-25996, CVE-2024-25997, CVE-2024-25998, CVE-2024-25999, CVE-2024-26000, CVE-2024-26001, CVE-2024-26002, CVE-2024-26003, CVE-2024-26004, CVE-2024-26005, CVE-2024-26288

VDE-2024-011

## Vulnerability Description

CVE-2024-25994
The exploit leverages vulnerabilities in the functionality to upload a script file.

CVE-2024-25995
The exploit leverages vulnerabilities to modify configuration and to perform a remote code execution.



...

CVE-2024-25996
The exploit introduces an insecure firewall rule to perform remote code execution.

CVE-2024-25997, CVE-2024-25998, CVE-2024-25999
The exploit combines multiple attacks, including a Man-In-The-Middle (MITM) attack, restricted file write, command injection, and privilege escalation, to perform remote code execution.

CVE-2024-26000, CVE-2024-26001, CVE-2024-26002
The exploit uses improper input validation in the MQTT handler to execute memory reads and memory writes to perform remote code execution.

CVE-2024-26003, CVE-2024-26004, CVE-2024-26005
The exploit uses malformed HomePlug packets to crash the ControllerAgent service and, on teardown, leverages a use-after-free to perform remote code execution.

CVE-2024-26288
An unauthenticated remote attacker can influence the communication due to the lack of encryption of sensitive data in OCPP1.6J via a MITM. Charging is not affected.

## Affected products

| Article no | Article | Affected versions |
|---|---|---|
| 1139022 | CHARX SEC-3000 | <= 1.5.0 |
| 1139018 | CHARX SEC-3050 | <= 1.5.0 |
| 1139012 | CHARX SEC-3100 | <= 1.5.0 |
| 1138965 | CHARX SEC-3150 | <= 1.5.0 |

## Impact

CVE-2024-25994, CVE-2024-25996, CVE-2024-25997, CVE-2024-26000
These vulnerabilities can be exploited by a malicious attacker without local account to gain root privileges, which allows him to take over the device.

CVE-2024-26003
This vulnerability can be used by a malicious attacker without local account to perform remote code execution with the privileges of the ControllerAgent service.

Some of the Vulnerabilities represent a medium risk on their own, nevertheless chaining or combining these vulnerabilities can trigger an RCE that leads to the complete compromise of the device.

**Classification of Vulnerability**

CVE-2024-25994
Base Score: 5.3
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CWE: CWE-20: Improper Input Validation

CVE-2024-25995
Base Score: 9.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-306: Missing Authentication for Critical Function

CVE-2024-25996
Base Score: 5.3
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CWE: CWE-346: Origin Validation Error

CVE-2024-26288
Base Score: 8.7
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
CWE: CWE-319: Cleartext Transmission of Sensitive Information

CVE-2024-25997
Base Score: 5.3
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CWE: CWE-20: Improper Input Validation

CVE-2024-25998
Base Score: 7.3
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CWE: CWE-20: Improper Input Validation

CVE-2024-25999
Base Score: 8.4
Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-20: Improper Input Validation

CVE-2024-26000
Base Score: 5.9
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: CWE-20: Improper Input Validation

CVE-2024-26001
Base Score: 7.4
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H
CWE: CWE-20: Improper Input Validation

CVE-2024-26002
Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-20: Improper Input Validation

CVE-2024-26003
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-125: Out-of-bounds Read

CVE-2024-26004
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-824: Access of Uninitialized Pointer

CVE-2024-26005
Base Score: 4.8
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
CWE: CWE-459: Incomplete Cleanup

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

## Temporary Fix / 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 our application note.

Measures to protect network-capable devices with Ethernet connection

## Remediation

Phoenix Contact strongly recommends updating to firmware version v1.5.1 or higher, which fixes these vulnerabilities.

## Acknowledgement

These vulnerabilities were discovered as part of a PWN2OWN competition initiated by Trend Micro Zero Day Initiative (ZDI).
We kindly appreciate the coordinated disclosure of these vulnerabilities by ZDI and the finders:

- Jack Dates of RET2 Systems
- Alex Plaskett and McCaulay Hudson of NCC Group
- Peter Geissler, Rick De Jager, Carlo Meijer
- Tobias Scharnowski and Felix Buchmann of fuzzware.io
- Chris Anastasio and Fabius Watson

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

## History

V1.0 (2024-03-12): Initial publication