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

14 May 2024
2024/00003

Security Advisory for CHARX-SEC3xxx Charge controllers

Publication Date:	2024-05-14
Last Update:	2024-06-03
Current Version:	V1.1

Advisory Title

Multiple vulnerabilities have been discovered in the Firmware of CHARX SEC charge controllers.

Advisory ID

CVE-2024-28133,
CVE-2024-28134,
CVE-2024-28135,
CVE-2024-28136,
CVE-2024-28137
VDE-2024-019

Vulnerability Description

CVE-2024-28137: This exploit leverages a TOCTOU vulnerability to perform a privilege escalation and remote code execution.

CVE-2024-28134: This exploit performs a Man-in-the-Middle attack to extract a session token from an unencrypted connection.

CVE-2024-28135: This exploit uses a command injection vulnerability to send a POST-request which performs remote code execution.

Registered office: Blomberg
Distr. court Lemgo HRA 3746
Personally liable partner:
Phoenix Contact Verwaltungs-GmbH
Management office Blomberg
Distr. court Lemgo HRB 10904
Statutory seat Vaduz/Liechtenstein
Comm. reg. FL-0002.700.066-3

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz
Chairman of the Advisory Board:
Dr. Dipl.-Ing. Eberhard Veit

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

CVE-2024-28133: This exploit performs privilege escalation using an untrusted search path vulnerability.

CVE-2024-28136: This exploit configures an attacker-controlled server as OCPP backend and uses a command injection vulnerability which is triggered by a command sent by the backend, to gain root privileges and perform remote code execution.

Affected products

Article no	Article	Affected versions
1139022	CHARX SEC-3000	<= 1.5.1
1139018	CHARX SEC-3050	<= 1.5.1
1139012	CHARX SEC-3100	<= 1.5.1
1138965	CHARX SEC-3150	<= 1.5.1

Impact

CVE-2024-28137: The exploit allows a local user to gain root privileges, which allows them to take over the device.

CVE-2024-28134: The exploit allows an attacker without local account to get access to the web-based management with the privileges of the currently logged in user.

CVE-2024-28135: The exploit allows a user of the web-based management to perform remote code execution on the device as a user with low privileges.

CVE-2024-28133: The exploit allows a local user on the device to perform privilege escalation to gain root privileges.

CVE-2024-28136: When the OCPP management port is opened, the exploit allows an attacker without local account to gain root privileges and perform remote code execution.

Classification of Vulnerability

CVE-2024-28133
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-426: Untrusted Search Path

CVE-2024-28134
Base Score: 7.0
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H
CWE: CWE-319: Cleartext Transmission of Sensitive Information

...

CVE-2024-28135
Base Score: 4.3
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE: CWE-20: Improper Input Validation

CVE-2024-28136
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-2024-28137
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-367: Time-of-check Time-of-use (TOCTOU) Race Condition

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 upgrading affected charge controllers to firmware version 1.6 or higher which fixes these vulnerabilities.

Acknowledgement

These vulnerabilities were discovered by Trend Micro's Zero Day Initiative and SinSinology
We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

For CVE-2024-28133, CVE-2024-28134, CVE-2024-28135 Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam) working with Trend Micro Zero Day Initiative.
For CVE-2024-28136 @ByteInsight working with Trend Micro Zero Day Initiative.
For CVE-2024-28137 Todd Manning working with Trend Micro Zero Day Initiative.

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

History

V1.0 (2024-05-14): Initial publication
V1.1 (2024-06-03): Acknowledgements extended