VDE-2026-008: Phoenix Contact: Multiple vulnerabilities in the firmware of CHARX SEC3xxx charging controllers

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Thu Jul 30 10:00:00 CEST 2026	Engine: 2.5.44
Current release date: Thu Jul 30 10:00:00 CEST 2026	Build Date: Mon Jul 27 06:11:18 CEST 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 9.8	Severity: Critical
Original language:	Language: en-GB
Also referred to: VDE-2026-008, PCSA-2026-00006	

Summary

Multiple vulnerabilities have been identified in the firmware of CHARX SEC-3xxx EV charging controllers, including the CHARX SEC-3000, SEC-3050, SEC-3100, and SEC-3150 models. The flaws could allow attackers to compromise the devices remotely, resulting in a complete loss of confidentiality, integrity, and availability.

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 recommends updating affected devices to firmware version 1.9.1, which addresses these vulnerabilities. The updated firmware will be made available as soon as possible, but no later than August 12, 2026. Please check the download section of the respective product webpage for the availability of the fix.

Affected Product(s)

Article	Name	Affected	Fixed
1138965	CHARX SEC-3150	Firmware <FW 1.9.1	Firmware FW 1.9.1
1139012	CHARX SEC-3150	Firmware <FW 1.9.1	Firmware FW 1.9.1
1139018	CHARX SEC-3050	Firmware <FW 1.9.1	Firmware FW 1.9.1
1139022	CHARX SEC-3000	Firmware <FW 1.9.1	Firmware FW 1.9.1

Acknowledgments

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

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

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- pcsa-2026-00006 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2026-008: Phoenix Contact: Multiple vulnerabilities in the firmware of CHARX SEC3xxx charging controllers - HTML (SELF): https://certvde.com/en/advisories/VDE-2026-008
- VDE-2026-008: Phoenix Contact: Multiple vulnerabilities in the firmware of CHARX SEC3xxx charging controllers - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-008.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
1.0.0	Thu Jul 30 10:00:00 CEST 2026	Initial revision.

Sharing rules

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

Vulnerability Details

Missing authentication for MQTT Broker (CVE-2026-44090)

CVE Description

Due to missing authentication, an unauthenticated remote attacker may access the MQTT broker, which is only protected from external access by a firewall. This may lead to the device being fully compromised.

CWE:	CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Giuseppe Cali (@_gcali) from Team Zeroshi for reporting.

References

- CVSS v4.0 Score: 9.3 / Critical (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Creation of a new configuration by posting a malicious ID to MQTT (CVE-2026-44091)

CVE Description

An unauthenticated remote attacker can post a malicious ID to the MQTT Broker results in the creation of a new configuration entry in the system configuration. This may lead to integrity and availability loss.

CWE:	CWE-501: Trust Boundary Violation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Giuseppe Cali (@_gcali) from Team Zeroshi for reporting.

References

- CVSS v4.0 Score: 8.8 / High (EXTERNAL):
  https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N

Missing input validation / stripping of CRLF characters in SystemConfigManager (CVE-2026-44092)

CVE Description

An unauthenticated remote attacker can inject malicious input into the ModbusServer application because it does not validate the input it fetches from MQTT. This may lead to integrity and availability loss.

CWE:	CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	9.1

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Giuseppe Cali (@_gcali) from Team Zeroshi for reporting.

References

- CVSS v4.0 Score: 8.8 / High (EXTERNAL):
  https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N

Local Privilege Escalation vulnerability in /etc/init.d/user-applications via user-application start script (CVE-2026-44093)

CVE Description

A local privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Giuseppe Cali (@_gcali) from Team Zeroshi for reporting.

References

- CVSS v4.0 Score: 8.5 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

Fallback to second RAUC slot with default credentials (CVE-2026-44094)

CVE Description

An unauthenticated remote attacker can enforce the system to fall back to a firmware partition with an insecure configuration including default credentials. This could allow the attacker to gain SSH access to the system as an unprivileged user "user-app". Charging could be interrupted.

CWE:	CWE-636: Not Failing Securely ('Failing Open')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Giuseppe Cali (@_gcali) from Team Zeroshi for reporting.

References

- CVSS v4.0 Score: 8.3 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/

Local Privilege Escalation via Network scripts (CVE-2026-44095)

CVE Description

A privilege escalation vulnerability in a script used for network configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Hyeongseok Lee (@fluorite_pwn), Yunje Shin (@YunjeShin), Chaeeul Hyun (@yskm_Gunter), Ingyu Yang (@Mafty5275), Hoseok Kang (@cl4y419), Seungyeon Park (@vvsy46), Wonjun Choi (@won6_choi) from BoB::Takedown for reporting.
- Piotr Ptaszek, Mateusz Wójcik from TrendAI Zero Day Initiative for reporting.

References

- CVSS v4.0 Score: 8.5 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

udhcpc Privilege Escalation (CVE-2026-44096)

CVE Description

A privilege escalation vulnerability in udhcpc allows a local user "charx-web" to execute arbitrary commands as root, resulting in full system compromise.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Hyeongseok Lee (@fluorite_pwn), Yunje Shin (@YunjeShin), Chaeeul Hyun (@yskm_Gunter), Ingyu Yang (@Mafty5275), Hoseok Kang (@cl4y419), Seungyeon Park (@vvsy46), Wonjun Choi (@won6_choi) from BoB::Takedown for reporting.

References

- CVSS v4.0 Score: 8.5 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

File Upload vulnerability (CVE-2026-44097)

CVE Description

A low-privileged remote attacker with "operator" access can upload arbitrary files via the REST endpoint intended for firmware updates, resulting in persistent storage of attacker-controlled files and potentially exhausting resources, which might lead to Denial-of-Service.

CWE:	CWE-434: Unrestricted Upload of File with Dangerous Type

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H	7.1
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H	7.1
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H	7.1
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H	7.1

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Hyeongseok Lee (@fluorite_pwn), Yunje Shin (@YunjeShin), Chaeeul Hyun (@yskm_Gunter), Ingyu Yang (@Mafty5275), Hoseok Kang (@cl4y419), Seungyeon Park (@vvsy46), Wonjun Choi (@won6_choi) from BoB::Takedown for reporting.

References

- CVSS v4.0 Score: 5.3 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/

OS Command Injection in OCPP Agent via charge_box_id (CVE-2026-44098)

CVE Description

This vulnerability allows an unauthenticated remote attacker with control over the OCPP backend via firewall-bypass to perform an OS command injection, resulting in the execution of arbitrary commands as the limited user charx-oa. Charging could be interrupted.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	8.6

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- 78ResearchLab RS (Red Spider) Team for reporting.

References

- CVSS v4.0 Score: 8.8 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/

Local Privilege Escalation via pppd password injection (CVE-2026-44099)

CVE Description

A privilege escalation vulnerability in the system configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- 78ResearchLab RS (Red Spider) Team for reporting.

References

- CVSS v4.0 Score: 8.5 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

JupiCore charging point reconfiguration without auth (CVE-2026-44100)

CVE Description

The CHARX JupiCore service allows an unauthenticated remote attacker to reconfigure charging points. This can lead to disclosure of charging point UIDs, Denial-of-Service and files tampering.

CWE:	CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	9.4
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	9.4
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	9.4
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	9.4

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Bongeun Koo (@kiddo_pwn), Evangelos Daravigkas (@freddo_1337) from Team DDOS for reporting.

References

- CVSS v4.0 Score: 8.8 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N

OCPP reconfiguration vulnerability (CVE-2026-44101)

CVE Description

Due to missing authentication the CHARX OCPP Agent service allows an unauthenticated remote attacker to reconfigure the backend connection. This can lead to Denial-of-Service and confidential data being disclosed to the attacker.

CWE:	CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Bongeun Koo (@kiddo_pwn), Evangelos Daravigkas (@freddo_1337) from Team DDOS for reporting.

References

- CVSS v4.0 Score: 9.3 / Critical (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

OCPP Firmware download is not properly locked (CVE-2026-44102)

CVE Description

An unauthenticated remote attacker can trigger a firmware update download via the OCPP backend by supplying an invalid firmware file. This will cause the file to remain accessible for a short period before it is deleted due to improper locking during the cleanup process.

CWE:	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Bongeun Koo (@kiddo_pwn), Evangelos Daravigkas (@freddo_1337) from Team DDOS for reporting.

References

- CVSS v4.0 Score: 6.9 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N

JupiCore does not perform validation of firmware (CVE-2026-44103)

CVE Description

An unauthenticated remote attacker can inject malicious firmware into the internal charging module because the JupiCore service transmits firmware updates without performing integrity or verification check. Successful exploitation may compromise the integrity of the affected device. This vulnerability could be used in chain with CVE-2026-44104.

CWE:	CWE-434: Unrestricted Upload of File with Dangerous Type

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	5.3

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Bongeun Koo (@kiddo_pwn), Evangelos Daravigkas (@freddo_1337) from Team DDOS for reporting.

References

- CVSS v4.0 Score: 6.9 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N

ControllerAgent does not perform validation of firmware (CVE-2026-44104)

CVE Description

The firmware update process for the basemodule of the charging controller only validates the CRC32 checksum without cryptographic signature verification. This allows an unauthenticated remote attacker to install a modified firmware, resulting in full system compromise.

CWE:	CWE-347: Improper Verification of Cryptographic Signature

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Bongeun Koo (@kiddo_pwn), Evangelos Daravigkas (@freddo_1337) from Team DDOS for reporting.

References

- CVSS v4.0 Score: 9.3 / Critical (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Local Privilege Escalation vulnerability in /etc/init.d/user-applications via customer website file (CVE-2026-44106)

CVE Description

A privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.

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
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Julien Cohen-Scali, Nabih Benazzouz, Hugo Leclercq from FuzzingLabs for reporting.

References

- CVSS v4.0 Score: 5.3 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

Cleartext password in logs (CVE-2026-44105)

CVE Description

The credentials for the local user "user-app" may be exposed in log files, potentially enabling a low-privileged local attacker with access to the logs to authenticate via SSH as the limited user "user-app". Charging could be interrupted.

CWE:	CWE-532: Insertion of Sensitive Information into Log File

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H	6.6
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H	6.6
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H	6.6
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H	6.6

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Julien Cohen-Scali, Nabih Benazzouz, Hugo Leclercq from FuzzingLabs for reporting.

References

- CVSS v4.0 Score: 5.8 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/S

Exposed Reboot via Modbus (CVE-2026-44107)

CVE Description

A reboot of the charging controller can be triggered via Modbus TCP without authentication. Therefore, when the Modbus functionality is enabled by opening the port that CharxModbusServer is listening, an unauthenticated attacker can perform a Denial-of-Service attack.

CWE:	CWE-749: Exposed Dangerous Method or Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Team PetoWorks for reporting.
- Hyeongseok Lee (@fluorite_pwn), Yunje Shin (@YunjeShin), Chaeeul Hyun (@yskm_Gunter), Ingyu Yang (@Mafty5275), Hoseok Kang (@cl4y419), Seungyeon Park (@vvsy46), Wonjun Choi (@won6_choi) from BoB::Takedown for reporting.
- 78ResearchLab RS (Red Spider) Team for reporting.

References

- CVSS v4.0 Score: 8.7 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N

Firewall bypass during shutdown (CVE-2026-44108)

CVE Description

Due to a flaw in the execution order of scripts during shutdown, the firewall is terminated prematurely during system shutdown. This creates a temporary window in which internal services may become externally accessible, potentially allowing an unauthenticated remote attacker to connect to these services, resulting in full system compromise.

CWE:	CWE-696: Incorrect Behavior Order

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Team PetoWorks for reporting.
- Hyeongseok Lee (@fluorite_pwn), Yunje Shin (@YunjeShin), Chaeeul Hyun (@yskm_Gunter), Ingyu Yang (@Mafty5275), Hoseok Kang (@cl4y419), Seungyeon Park (@vvsy46), Wonjun Choi (@won6_choi) from BoB::Takedown for reporting.
- 78ResearchLab RS (Red Spider) Team for reporting.

References

- CVSS v4.0 Score: 9.3 / Critical (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Command Injection in SCM (idledisconnect parameter) (CVE-2026-7849)

CVE Description

Due to improper neutralization of special elements, an unauthenticated remote attacker is able to inject a command into the system configuration which is subsequently executed as root.

CWE:	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
Firmware <FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1138965 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3150 Order number: 1139012 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3050 Order number: 1139018 (Download)
Firmware FW 1.9.1 installed on CHARX SEC-3000 Order number: 1139022 (Download)

Acknowledgments

- Team PetoWorks for reporting.

References

- CVSS v4.0 Score: 9.3 / Critical (EXTERNAL):
  https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N