VDE-2025-072: Phoenix Contact: Security Advisory for QUINT4-UPS EIP

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Oct 14 08:00:00 CEST 2025	Engine: 2.5.36
Current release date: Tue Oct 14 08:00:00 CEST 2025	Build Date: Thu Oct 02 12:44:33 CEST 2025
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 7.5	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2025-072, PCSA-2025-00013	

Summary

Multiple vulnerabilities were discovered in the firmware of QUINT4-UPS EIP devices that can be used by an unauthenticated remote attacker to perform Denial of Service attacks and to gather login credentials for the Webfrontend.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

Impact

A successful attack can lead to Denial of Service or exposure of credentials.

Mitigation

Affected devices 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

Starting with version VC:07, all newly shipped devices will include firmware updates that address four vulnerabilities: CVE-2025-41704, CVE-2025-41705, CVE-2025-41706, and CVE-2025-41707.

However, configuration of devices via unauthenticated Modbus/TCP remains possible in VC:07, as this protocol is a widely used standard in the industrial sector. As a result, VC:07 is still affected by CVE-2025-41703.

Product description

Uninterruptible power supplies with an EIP interface.

Product groups

Affected Products.

- QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07
- QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07
- QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07
- QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07
- QUINT4-UPS/24DC/24DC/5/EIP VC:07
- QUINT4-UPS/24DC/24DC/10/EIP VC:07
- QUINT4-UPS/24DC/24DC/20/EIP VC:07
- QUINT4-UPS/24DC/24DC/40/EIP VC:07

Fixed Products. (CVE-2025-41704, CVE-2025-41705, CVE-2025-41706, CVE-2025-41707)

- QUINT4-UPS/24DC/24DC/5/EIP VC:07
- QUINT4-UPS/24DC/24DC/10/EIP VC:07
- QUINT4-UPS/24DC/24DC/20/EIP VC:07
- QUINT4-UPS/24DC/24DC/40/EIP VC:07

Vulnerabilities

Phoenix Contact: UPS Shutdown via Unauthenticated Modbus Command (CVE-2025-41703)

Vulnerability Description

An unauthenticated remote attacker can cause a Denial of Service by turning off the output of the UPS via Modbus command.

CWE: CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/5/EIP VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/10/EIP VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/20/EIP VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
QUINT4-UPS/24DC/24DC/40/EIP VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Phoenix Contact: Unauthenticated Modbus Service DoS via Crafted Function Code (CVE-2025-41704)

Vulnerability Description

An unauthanticated remote attacker can perform a DoS of the Modbus service by sending a specific function and sub-function code without affecting the core functionality.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
QUINT4-UPS/24DC/24DC/5/EIP VC:07 Order number: 2906994 (Download)
QUINT4-UPS/24DC/24DC/10/EIP VC:07 Order number: 2907069 (Download)
QUINT4-UPS/24DC/24DC/20/EIP VC:07 Order number: 2907074 (Download)
QUINT4-UPS/24DC/24DC/40/EIP VC:07 Order number: 2907080 (Download)

Phoenix Contact: WebSocket Message Interception Leaks Webfrontend Credentials (CVE-2025-41705)

Vulnerability Description

An unauthenticated remote attacker (MITM) can intercept the websocket messages to gain access to the login credentials for the Webfrontend.

CWE: CWE-523: Unprotected Transport of Credentials

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8
QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	6.8

Fixed

Product
QUINT4-UPS/24DC/24DC/5/EIP VC:07 Order number: 2906994 (Download)
QUINT4-UPS/24DC/24DC/10/EIP VC:07 Order number: 2907069 (Download)
QUINT4-UPS/24DC/24DC/20/EIP VC:07 Order number: 2907074 (Download)
QUINT4-UPS/24DC/24DC/40/EIP VC:07 Order number: 2907080 (Download)

Phoenix Contact: Webserver Denial of Service through Malformed Content-Length (CVE-2025-41706)

Vulnerability Description

The webserver is vulnerable to a denial of service condition. An unauthenticated remote attacker can craft a special GET request with an over-long content-length to trigger the issue without affecting the core functionality.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
QUINT4-UPS/24DC/24DC/5/EIP VC:07 Order number: 2906994 (Download)
QUINT4-UPS/24DC/24DC/10/EIP VC:07 Order number: 2907069 (Download)
QUINT4-UPS/24DC/24DC/20/EIP VC:07 Order number: 2907074 (Download)
QUINT4-UPS/24DC/24DC/40/EIP VC:07 Order number: 2907080 (Download)

Phoenix Contact: WebSocket Handler Denial of Service (CVE-2025-41707)

Vulnerability Description

The websocket handler is vulnerable to a denial of service condition. An unauthenticated remote attacker can send a crafted websocket message to trigger the issue without affecting the core functionality.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
QUINT4-UPS/24DC/24DC/5/EIP VC:00<VC:07 Order number: 2906994	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/10/EIP VC:00<VC:07 Order number: 2907069	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/20/EIP VC:00<VC:07 Order number: 2907074	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3
QUINT4-UPS/24DC/24DC/40/EIP VC:00<VC:07 Order number: 2907080	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Fixed

Product
QUINT4-UPS/24DC/24DC/5/EIP VC:07 Order number: 2906994 (Download)
QUINT4-UPS/24DC/24DC/10/EIP VC:07 Order number: 2907069 (Download)
QUINT4-UPS/24DC/24DC/20/EIP VC:07 Order number: 2907074 (Download)
QUINT4-UPS/24DC/24DC/40/EIP VC:07 Order number: 2907080 (Download)

Acknowledgments

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

- CERTVDE for Coordination (see: https://certvde.com/en/)
- D. Blagojevic, S. Dietz, F. Koroknai, T. Weber from CyberDanube Security Research for Reporting

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- VDE-2025-072: Phoenix Contact: Security Advisory for QUINT4-UPS EIP - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-072/
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- PCSA-2025-00013 (EXTERNAL): https://phoenixcontact.com/psirt
- VDE-2025-072: Phoenix Contact: Security Advisory for QUINT4-UPS EIP - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-072.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Tue Oct 14 08:00:00 CEST 2025	Initial revision.

Sharing rules

TLP:WHITE

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