

VDE-2025-073: Phoenix Contact: Security Advisory for TC ROUTER and CLOUD CLIENT Industrial mobile network routers

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Jan 13 09:00:00 CET 2026	Engine: 2.5.41
Current release date: Tue Jan 13 09:00:00 CET 2026	Build Date: Thu Jan 08 11:01:51 CET 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 8.8	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2025-073, PCSA-2025-00014	

Summary

A code injection vulnerability at the upload-config endpoint in the firmware of TC ROUTER and CLOUD CLIENT Industrial Mobile network routers has been discovered that can be exploited by an high privileged attacker.

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 vulnerability can lead to a total loss of confidentiality, integrity and availability of the devices.

Mitigation

As this vulnerability can only be exploited by an authenticated high privileged user, Phoenix Contact recommends to strictly restrict administrative access to the device. The administrative use shall only import configuration files from trusted sources.

Remediation

Phoenix Contact recommends to upgrade to the latest firmware which will fix this vulnerability.

Product	Fixed Version
TC ROUTER 3002T-3G	3.08.8
TC ROUTER 2002T-3G	3.08.8
TC ROUTER 3002T-4G	3.08.8
TC ROUTER 3002T-4G GL	3.08.8
TC ROUTER 5004T-5G EU	1.06.23
TC ROUTER 3002T-4G VZW	3.08.8
TC ROUTER 3002T-4G ATT	3.08.8
TC ROUTER 2002T-4G	3.08.8
CLOUD CLIENT 1101T-TX/TX	3.07.7
TC CLOUD CLIENT 1002-4G ATT	3.08.8
TC CLOUD CLIENT 1002-TX/TX	3.07.7

Product Description

Industrial mobile network router.

Product groups

Affected products.

- Firmware <FW 3.08.8 installed on TC ROUTER 3002T-3G
- Firmware <FW 3.08.8 installed on TC ROUTER 2002T-3G
- Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G
- Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G GL
- Firmware <FW 1.06.23 installed on TC ROUTER 5004T-5G EU
- Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G VZW
- Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G ATT
- Firmware <FW 3.08.8 installed on TC ROUTER 2002T-4G
- Firmware <FW 3.07.7 installed on CLOUD CLIENT 1101T-TX/TX
- Firmware <FW 3.08.8 installed on TC CLOUD CLIENT 1002-4G ATT
- Firmware <FW 3.07.7 installed on TC CLOUD CLIENT 1002-TX/TX

Fixed products.

- Firmware 3.08.8 installed on TC ROUTER 3002T-3G
- Firmware 3.08.8 installed on TC ROUTER 2002T-3G
- Firmware 3.08.8 installed on TC ROUTER 3002T-4G
- Firmware 3.08.8 installed on TC ROUTER 3002T-4G GL
- Firmware 1.06.23 installed on TC ROUTER 5004T-5G EU
- Firmware 3.08.8 installed on TC ROUTER 3002T-4G VZW
- Firmware 3.08.8 installed on TC ROUTER 3002T-4G ATT
- Firmware 3.08.8 installed on TC ROUTER 2002T-4G
- Firmware 3.07.7 installed on CLOUD CLIENT 1101T-TX/TX
- Firmware 3.08.8 installed on TC CLOUD CLIENT 1002-4G ATT
- Firmware 3.07.7 installed on TC CLOUD CLIENT 1002-TX/TX

Vulnerabilities

Config-Upload Code Injection (CVE-2025-41717)

CVE Details

The config-upload endpoint can be exploited to inject arbitrary commands that are executed when polling the sock_server. The malicious config changes the root password and activates the service.

CVE Description

An unauthenticated remote attacker can trick a high privileged user into uploading a malicious payload via the config-upload endpoint, leading to code injection as root. This results in a total loss of confidentiality, availability and integrity due to improper control of code generation ('Code Injection').

CWE:	CWE-94: Improper Control of Generation of Code ('Code Injection')
Release date:	Tue Jan 13 12:00:00 CET 2026

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <FW 3.08.8 installed on TC ROUTER 3002T-3G Order number: 2702529	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 2002T-3G Order number: 2702531	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G Order number: 2702528	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G GL Order number: 1632697	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 1.06.23 installed on TC ROUTER 5004T-5G EU Order number: 1439475	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G VZW Order number: 2702532	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 3002T-4G ATT Order number: 2702533	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC ROUTER 2002T-4G Order number: 2702530	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.07.7 installed on CLOUD CLIENT 1101T-TX/TX Order number: 1221706	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.08.8 installed on TC CLOUD CLIENT 1002-4G ATT Order number: 2702888	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8
Firmware <FW 3.07.7 installed on TC CLOUD CLIENT 1002-TX/TX Order number: 2702885	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

Fixed

Product

Firmware 3.08.8 installed on TC ROUTER 3002T-3G
Order number: 2702529 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 2002T-3G
Order number: 2702531 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 3002T-4G
Order number: 2702528 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 3002T-4G GL
Order number: 1632697 ([Download](#))

Firmware 1.06.23 installed on TC ROUTER 5004T-5G EU
Order number: 1439475 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 3002T-4G VZW
Order number: 2702532 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 3002T-4G ATT
Order number: 2702533 ([Download](#))

Firmware 3.08.8 installed on TC ROUTER 2002T-4G
Order number: 2702530 ([Download](#))

Firmware 3.07.7 installed on CLOUD CLIENT 1101T-TX/TX
Order number: 1221706 ([Download](#))

Firmware 3.08.8 installed on TC CLOUD CLIENT 1002-4G ATT
Order number: 2702888 ([Download](#))

Firmware 3.07.7 installed on TC CLOUD CLIENT 1002-TX/TX
Order number: 2702885 ([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 for Reporting.

Phoenix Contact GmbH & Co. KG

Namespace: <https://phoenixcontact.com/psirt>

psirt@phoenixcontact.com

References

- PCSA-2025-00014 (EXTERNAL): <https://phoenixcontact.com/psirt>
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): <https://certvde.com/de/advisories/vendor/phoenixcontact/>
- VDE-2025-073: Phoenix Contact: Security Advisory for TC ROUTER and CLOUD CLIENT Industrial mobile network routers - HTML (SELF): <https://certvde.com/en/advisories/VDE-2025-073>
- VDE-2025-073: Phoenix Contact: Security Advisory for TC ROUTER and CLOUD CLIENT Industrial mobile network routers - CSAF (SELF): <https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2025-073.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	Tue Jan 13 09:00:00 CET 2026	Initial Revision

Sharing rules

TLP:WHITE

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