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

100 years of passion for technology and innovation

08 August 2023
2023/00011

Security Advisory for TC ROUTER and TC CLOUD CLIENT

Publication Date: 2023-08-08
Last Update: 2023-08-08
Current Version: V1.0

Advisory Title

Two vulnerabilities have been discovered in the firmware of TC ROUTER and TC CLOUD CLIENT devices.

Advisory ID

CVE-2023-3526
CVE-2023-3569
VDE-2023-017

Vulnerability Description

A reflected cross-site scripting vulnerability can be triggered in the license viewer of the device. This can be used to execute malicious code in the context of the user's browser or to copy cookies.

By abusing the configuration file upload functionality of the device, it is possible to provoke high CPU load which may slow down other processes.

...

Affected products

Article no	Article	Affected versions	Fixed version
2702528	TC ROUTER 3002T-4G	< 2.07.2	Download
2702533	TC ROUTER 3002T-4G ATT	< 2.07.2	Download
2702532	TC ROUTER 3002T-4G VZW	< 2.07.2	Download
2702886	TC CLOUD CLIENT 1002-4G	< 2.07.2	Download
2702888	TC CLOUD CLIENT 1002-4G ATT	< 2.07.2	Download
2702887	TC CLOUD CLIENT 1002-4G VZW	< 2.07.2	Download
1221706	CLOUD CLIENT 1101T-TX/TX	< 2.06.10	Download

Impact

An attacker could embed a link on a page controlled by him that includes malicious scripts and points to the license viewer page. These scripts are executed in a victim's browser when they open the page containing the vulnerable field.

An authenticated attacker could use the file upload function to upload a crafted XML to cause a denial of service.

Classification of Vulnerability

CVE-2023-3526
Base Score: 9.6
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
CWE: CWE-79

CVE-2023-3569
Base Score: 4.9
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-776

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 the latest available firmware version, which fixes these vulnerabilities.

Acknowledgement

These vulnerabilities were discovered by A. Resanovic and S. Stockinger at St. Pölten UAS and coordinated by T. Weber of CyberDanube Security Research.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

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

History

V1.0 (2023-08-08): Initial publication