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

07 March 2023
2022/00009

Security Advisory for TC ROUTER and CLOUD CLIENT

Publication Date: 2023-03-07
Last Update: 2023-03-07
Current Version: V1.0

Advisory Title

Two Vulnerabilities have been discovered in TC ROUTER 4000 series and CLOUD CLIENT 2000 series up to firmware version 4.5.7x.107

Advisory ID

CVE-2023-0861
CVE-2023-0862
VDE-2022-053

Vulnerability Description

The web administration interface is vulnerable for **authenticated admin users** to path traversals, which could lead to arbitrary file uploads or deletion. Unvalidated user input also enables execution of OS commands.

...

Affected products

Article no	Article	Affected versions	Fixed version
1234352	TC ROUTER 4002T-4G EU	< 4.5.72.107	Download
1234353	TC ROUTER 4102T-4G EU WLAN	< 4.5.72.107	Download
1234354	TC ROUTER 4202T-4G EU WLAN	< 4.5.72.107	Download
1234355	CLOUD CLIENT 2002T-4G EU	< 4.5.73.107	Download
1234360	CLOUD CLIENT 2002T-WLAN	< 4.5.73.107	Download
1234357	CLOUD CLIENT 2102T-4G EU WLAN	< 4.5.73.107	Download

Impact

The web interface is available only after authentication. An authorized admin user could use these vulnerabilities to execute arbitrary commands, upload arbitrary files or delete files from the device. This may lead to the device no longer functioning properly.

Classification of Vulnerability

Arbitrary Command Injection
CVE-2023-0861
Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-77: Improper Neutralization of Special Elements used in a Command

Arbitrary File Upload / Removal
CVE-2023-0862
Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory

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

The vulnerability is fixed in firmware version 4.6.7x.101. We strongly recommend all affected users to upgrade to this or a later version.

Acknowledgement

This vulnerability was discovered and reported by ONEKEY.

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 (2023-03-07): Initial publication