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

04 March 2020
300472147/pbsa56

Security Advisory for TC ROUTER & TC CLOUD CLIENT devices

Advisory Title

Multiple vulnerabilities have been discovered in the TC ROUTER & TC CLOUD CLIENT firmware.

Advisory ID

CVE-2017-16544
CVE-2020-9435
CVE-2020-9436
VDE-2020-003

Vulnerability Description

CVE-2017-16544
In BusyBox through 1.27.2, the tab auto complete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal.

CVE-2020-9436
An authenticated command injection vulnerability can be triggered by issuing a POST request to an CGI program which is available on the web interface.

CVE-2020-9435
The device contains a hardcoded certificate which can be used to run the web service. Impersonation, man-in-the-middle or passive decryption attacks are possible if the generic certificate is not replaced by a device specific certificate during installation.

Affected products

Article name	Article number	Affected versions
TC ROUTER 3002T-4G	2702528	<= 2.05.3
TC ROUTER 3002T-4G	2702530	<= 2.05.3
TC ROUTER 2002T-3G	2702529	<= 2.05.3
TC ROUTER 2002T-3G	2702531	<= 2.05.3
TC ROUTER 3002T-4G VZW	2702532	<= 2.05.3
TC ROUTER 3002T-4G ATT	2702533	<= 2.05.3

Article name	Article number	Affected versions
TC CLOUD CLIENT 1002-4G	2702886	<= 2.03.17
TC CLOUD CLIENT 1002-4G VZW	2702887	<= 2.03.17
TC CLOUD CLIENT 1002-4G ATT	2702888	<= 2.03.17

Article name	Article number	Affected versions
TC CLOUD CLIENT 1002-TXTX	2702885	<= 1.03.17

Impact

CVE-2017-16544
This Vulnerability could potentially result in code execution, arbitrary file writes, or other attacks. The impact of this vulnerability on the device is limited because shell access is only possible with administrator privileges.

CVE-2020-9436
An attacker can abuse this vulnerability to compromise the operating system of the device by injecting system commands.

CVE-2020-9435
These attacks could allow an attacker to gain access to sensitive information like admin credentials, configuration parameters or status information and use them in further attacks.

Classification of Vulnerability

CVE-2017-16544
Base Score: 8.8
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2020-9436
Base Score: 7.2
Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2020-9435
Base Score: 9.1
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Mitigation

The pre-installed generic X.509 certificate should be renewed or replaced by an individual certificate during initial configuration. For details on replacing this certificate please refer to the user manual on page 51 et seq. Press “renew” to create a new self-signed device certificate or upload a user specific certificate with the upload dialog.

To avoid the manual generation of an individual certificate, the devices will be shipped with individual certificates starting with a future release.

Remediation

Phoenix Contact strongly recommended to update affected devices to newest Firmware version:

Article name	Article number	Fixed version	Link
TC ROUTER 3002T-4G	2702528	2.05.4	download
TC ROUTER 3002T-4G	2702530	2.05.4	download
TC ROUTER 2002T-3G	2702529	2.05.4	download
TC ROUTER 2002T-3G	2702531	2.05.4	download
TC ROUTER 3002T-4G VZW	2702532	2.05.4	download
TC ROUTER 3002T-4G ATT	2702533	2.05.4	download

Article name	Article number	Fixed version	Link
TC CLOUD CLIENT 1002-4G	2702886	2.03.18	download
TC CLOUD CLIENT 1002-4G VZW	2702887	2.03.18	download
TC CLOUD CLIENT 1002-4G ATT	2702888	2.03.18	download

Article name	Article number	Fixed version	Link
TC CLOUD CLIENT 1002-TXTX	2702885	1.03.18	download

...

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 against unauthorized access

Acknowledgement

This vulnerability was discovered and reported by Thomas Weber, SEC Consult Vulnerability Lab.