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 June 2021
300510142

Security Advisory for PLCNext, ILC 2050 BI, FL MGUARD DM UNLIMITED, TC ROUTER und CLOUD CLIENT products

Advisory Title

A Denial of Service and a CA Check Problem have been identified in multiple openSSL 1.1.1 versions, which are utilized in the Phoenix Contact products listed below.

Advisory ID

CVE-2021-3449
CVE-2021-3450
VDE-2021-025

Vulnerability Description

CVE-2021-3449: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client (CWE-476).

CVE-2021-3450: An error in the implementation of an additional security check of the certificates present in a certificate chain may cause an override situation that leads to a failed certificate check (CWE-295).

Affected products

Article no	Article	Affected versions	Fixed version
1151412	AXC F 1152	<= 2021.0 LTS	2021.0.5 LTS
2404267	AXC F 2152	<= 2021.0 LTS	2021.0.5 LTS
1069208	AXC F 3152	<= 2021.0 LTS	2021.0.5 LTS
1051328	RFC 4072S	<= 2021.0 LTS	2021.0.5 LTS
1046568	AXC F 2152 Starterkit	<= 2021.0 LTS	2021.0.5 LTS
1188165	PLCnext Technology Starterkit	<= 2021.0 LTS	2021.0.5 LTS
2981974	FL MGUARD DM UNLIMITED	<= 1.12	1.13
2702528	TC ROUTER 3002T-4G	<= 2.06.3	2.06.5
2702529	TC ROUTER 2002T-3G	<= 2.06.3	2.06.5
2702530	TC ROUTER 3002T-4G	<= 2.06.3	2.06.5
2702531	TC ROUTER 2002T-3G	<= 2.06.3	2.06.5
2702532	TC ROUTER 3002T-4G VZW	<= 2.06.3	2.06.5
2702533	TC ROUTER 3002T-4G ATT	<= 2.06.3	2.06.5
1221706	CLOUD CLIENT 1101T-TX/TX	<= 2.06.4	2.06.5
1234352	TC ROUTER 4002T-4G EU	<= 4.5.72.100	End of Q2 2021
1234353	TC ROUTER 4102T-4G EU WLAN	<= 4.5.72.100	End of Q2 2021
1234354	TC ROUTER 4202T-4G EU WLAN	<= 4.5.72.100	End of Q2 2021
1234355	CLOUD CLIENT 2002T-4G EU	<= 4.5.72.100	End of Q2 2021
1234360	CLOUD CLIENT 2002T-WLAN	<= 4.5.72.100	End of Q2 2021
1234357	CLOUD CLIENT 2102T-4G EU WLAN	<= 4.5.72.100	End of Q2 2021
2403160	ILC 2050 BI	<= 1.5.1	End of Q2 2021
2404671	ILC 2050 BI-L	<= 1.5.1	End of Q2 2021
1110435	SMARTRTU AXC SG	<= V1.6.0.1	End of Q3 2021
1264328	SMARTRTU AXC IG	<= V1.0.0.0	End of Q3 2021
1264327	ENERGY AXC PU	<= V4.10.0.0	End of Q3 2021

Impact

CVE-2021-3449: A malicious Attacker could use this vulnerability to execute a denial-of-service attack against services utilizing openSSL.

CVE-2021-3450: In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose.

Note: ILC 20250 is only affected by CVE-2021-3449

Classification of Vulnerability

CVE-2021-3449:
Base Score: 5.9
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2021-3450:

Base Score: 7.4
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

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 firmware mentioned in the list of affected products, which fixes this vulnerability.

A fix for ILC 2050, and some TC ROUTER and CLOUD CLIENT devices will be available end of Q2 2021. This advisory will be updated as soon as the fixes are available for download.

Acknowledgement

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.