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
300509941

Security Advisory for PLCNext, SMARTRTU AXC, CHARX control modular and EEM-SB37x

Advisory Title

At Pengutronix RAUC update client prior to version 1.5 a Time-of-Check Time-of-Use vulnerability was discovered. A vulnerable RAUC version is used in the current firmware of the products listed below.

Advisory ID

CVE-2020-25860
VDE-2021-024

Vulnerability Description

The vulnerability is a Time-of-Check-Time-of-Use (CWE-367) issue which allows an attacker with access to the firmware update file to overwrite it after it has been verified (but before installation is completed), which consequently allows installing an arbitrary firmware update, bypassing the cryptographic signature check mechanism.

Personally liable partner:	Group Executive Board:	Deutsche Bank AG	Commerzbank AG
Phoenix Contact Verwaltungs GmbH	Frank Stührenberg (CEO)	(BLZ 360 700 50) 226 2665 00	(BLZ 476 400 51) 226 0396 00
Amtsgericht Lemgo HRB 5273	Dirk Görlitzer, Torsten Janwlecke	BIC: DEUTDEDEXXX	BIC: COBADEFFXXX
Kom. Ges. Amtsgericht Lemgo HRA 3746	Ulrich Leidecker	IBAN:	IBAN:
	Frank Possel-Dölken, Axel Wachholz	DE93 3607 0050 0226 2665 00	DE31 4764 0051 0226 0396 00

...

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
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
1158951	EEM-SB370-C	<= 2021.02.01	End of Q3 2021
1158947	EEM-SB371-C	<= 2021.02.01	End of Q3 2021
1139022	CHARX control modular 3000	<= V1.0.11	End of Q3 2021
1139018	CHARX control modular 3050	<= V1.0.11	End of Q3 2021
1139012	CHARX control modular 3100	<= V1.0.11	End of Q3 2021
1138965	CHARX control modular 3150	<= V1.0.11	End of Q3 2021

Impact

An attacker who can modify the update file just before it is reopened can install arbitrary code on the device.

Classification of Vulnerability

Base Score: 8.8
Vector: CVSS: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

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.

For EEM-SB370, EEM-SB371 and CHARX control modular the fix will be available until end of Q3 2021. This advisory will be updated as soon the fix is available.

Acknowledgement

...

This vulnerability was discovered and reported to Pengutronix by Vdoo.

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.