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

12 April 2022
300547948

Security Advisory: Multiple Linux component vulnerabilities fixed in latest AXC F x152 and RFC 4072S LTS release

Advisory Title

PLCnext Control Firmware < 2022.0.3 LTS contains multiple Linux component vulnerabilities.

Advisory ID

CVE-2021-42385, CVE-2021-46143, CVE-2022-23990, CVE-2022-23852, CVE-2022-22827, CVE-2022-22826, CVE-2022-22825, CVE-2022-22824, CVE-2022-22823, CVE-2022-22822, CVE-2021-45960, CVE-2021-45117, CVE-2021-3712, CVE-2021-3711, CVE-2021-41990, CVE-2021-45079, CVE-2016-20012, CVE-2020-15078, CVE-2021-3580, CVE-2021-20305, CVE-2021-40330, CVE-2021-35942, CVE-2020-6096, CVE-2020-29562, CVE-2021-20231, CVE-2021-20232, CVE-2020-24659, CVE-2019-17498, CVE-2021-3517, CVE-2021-3518, CVE-2021-3537, CVE-2020-10878, CVE-2020-10543, CVE-2020-12723, CVE-2021-20193, CVE-2021-23017, CVE-2019-20892, CVE-2021-43618, CVE-2019-20907, CVE-2021-22946, CVE-2020-8169, CVE-2021-22926, CVE-2020-8177, CVE-2018-1000500, CVE-2021-22922, CVE-2021-22947, CVE-2021-22897, CVE-2021-22925, CVE-2021-22923, CVE-2021-22898, CVE-2021-42374, CVE-2021-42386, CVE-2021-42380, CVE-2021-42381, CVE-2021-42379, CVE-2021-42384, CVE-2021-42378, CVE-2021-42382, CVE-2019-18276, CVE-2021-21300
VDE-2022-010

Vulnerability Description

PLCnext Control devices are certified according to IEC 62443-4-1 and IEC 62443-4-2.
This certification requires that all third-party components used in the firmware are regularly checked for known vulnerabilities.

Firmware components in version 2021.06 had already been updated. For the 2022.0 LTS version more firmware components have been updated implicitly fixing the vulnerabilities listed. The vulnerabilities listed above have not been individually verified in terms of actual impact and/or limitations in combination with the affected products listed. The current LTS release 2022.0 LTS contains updates of integrated third-party libraries, SDKs and other third-party software to address these issues nevertheless.

Affected products

Article no	Article	Affected versions	Fixed Version
2404267	AXC F 2152	< 2022.0.3 LTS	Download
1151412	AXC F 1152	< 2022.0.3 LTS	Download
1069208	AXC F 3152	< 2022.0.5 LTS	Download
1051328	RFC 4072S	< 2022.0.5 LTS	Download

Impact

Availability, integrity, or confidentiality of the AXC F x152 or RFC 4072S might be compromised by attacks using these vulnerabilities.

Classification of Vulnerability

For detailed information according to the CVSS score please refer to VDE-2022-010.

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

Update to Firmware Release 2022.0.3 LTS or higher.
Update to PLCnext Engineer Release 2022.0.1 LTS or higher.
Please check the PHOENIX CONTACT PSIRT webpage for further updates of this advisory.

Acknowledgement

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

Update V1.1 2022-04-28

- Added RFC 4072S
- Release version for AXC 3152 corrected

...

Annex 1: Fixed Vulnerabilities

SSL

– CVE-2021-3712
– CVE-2021-3711
– Deprecated encryption versions “TLSv1.0” and
“TLSv1.1” were allowed over certain ports.

Strongswan

– CVE-2021-41990
– CVE-2021-45079

Open SSH

– CVE-2016-20012

Open VPN

– CVE-2020-15078

Nettle

– CVE-2021-3580
– CVE-2021-20305

GIT

– CVE-2021-40330
– CVE-2021-21300

GLIBC

– CVE-2021-35942
– CVE-2020-6096
– CVE-2020-29562

GNUTLS

– CVE-2021-20231
– CVE-2021-20232
– CVE-2020-24659

LIBSSH2

– CVE-2019-17498

LIBXML2

– CVE-2021-3517
– CVE-2021-3518
– CVE-2021-3537

PERL

– CVE-2020-10878
– CVE-2020-10543
– CVE-2020-12723

TAR

– CVE-2021-20193

NGINX

– CVE-2021-23017

NET-SNMP

– CVE-2019-20892

GMP

– CVE-2021-43618

Python

– CVE-2019-20907

LIBEXPAT

– CVE-2021-45960
– CVE-2022-22824
– CVE-2022-22823
– CVE-2022-22822
– CVE-2022-22825

...

– CVE-2021-46143
– CVE-2022-22826
– CVE-2022-22827
– CVE-2022-23852
– CVE-2022-23990

CURL

– CVE-2021-22946
– CVE-2020-8169
– CVE-2021-22926
– CVE-2020-8177
– CVE-2021-22922
– CVE-2021-22947
– CVE-2021-22897
– CVE-2021-22925
– CVE-2021-22923
– CVE-2021-22898

Busybox

– CVE-2021-42374
– CVE-2021-42386
– CVE-2021-42380
– CVE-2021-42381
– CVE-2021-42379
– CVE-2021-42384
– CVE-2021-42378
– CVE-2021-42382
– CVE-2021-42385
The documented CVEs were not fixed via an update of busybox. Instead, the affected busybox components have been removed
– CVE-2018-1000500

OPC UA

– CVE-2021-45117

BASH

– CVE-2019-18276