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

11 October 2022
2022/00003

Security Advisory: Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2022.0.8 LTS

Publication Date: 2022-10-11
Last Update: 2022-11-22
Current Version: V1.1

Advisory Title

Update for PLCnext Firmware containing fixes for recent vulnerability findings in Linux components and security enhancements.

Advisory ID

VDE-2022-046

Vulnerability Description

PLCnext Control AXC F x152 is 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.

Vulnerabilities are fixed for all PLCnext Control targets described in the table below. The fixed vulnerabilities are enlisted in Annex 1.

Affected products

Article no	Article	Affected versions	Fixed Version
1151412	AXC F 1152	< 2022.0.8 LTS	Download
2404267	AXC F 2152	< 2022.0.8 LTS	Download
1069208	AXC F 3152	< 2022.0.8 LTS	Download
1051328	RFC 4072S	< 2022.0.8 LTS	Download
1246285	BPC 9102S	< 2022.0.8 LTS	Download

...

1185416	EPC 1502	< 2022.0.7 LTS	Download
1185423	EPC 1522	< 2022.0.7 LTS	Download
1264327	ENERGY AXC PU	< V04.14.00.00	V04.14.00.00
1110435	SMARTRTU AXC SG	< V01.09.00.00	End of Q1 2023

Impact

Availability, integrity, or confidentiality of the PLCnext Control might be compromised by attacks using these vulnerabilities.

Classification of Vulnerability

For detailed information to the CVEs like CVSS scores please refer to VDE-2022-046

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 the latest LTS Firmware Release.
Update to the latest LTS PLCnext Engineer Release.
Please check our PSIRT webpage for further Updates of this Advisory.

Acknowledgement

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

History

V1.0 (2022-10-11): Initial publication
V1.X (2022-11-22): Two devices (ENERGY AXC PU, SMARTRTU AXC SG) added

Annex 1: Fixed Vulnerabilities

Changes in Firmware 2022.0.7

Busybox

– CVE-2022-28391

LIBEXPAT

– CVE-2022-25235
– CVE-2022-25236
– CVE-2022-25313
– CVE-2022-25314
– CVE-2022-25315

LIBXML

– CVE-2022-29824
– CVE-2022-23308

OpenSSL

– CVE-2022-0778

OpenVPN

– CVE-2022-0547

Vim

– CVE-2022-1381
– CVE-2022-1420
– CVE-2022-1733
– CVE-2022-1796
– CVE-2022-1621
– CVE-2022-1616
– CVE-2022-1619
– CVE-2022-1629
– CVE-2022-1735
– CVE-2022-1769
– CVE-2022-1785
– CVE-2022-1620
– CVE-2022-1674
– CVE-2022-1771
– CVE-2022-1886
– CVE-2022-1851
– CVE-2022-1898
– CVE-2022-1720

ZLib

– CVE-2018-25032

OPC UA

Unified Automation reported several security risks for the OPC UA SDK 1.7.6 and before. All reported issues are fixed with the update of OPC UA SDK version 1.7.7.

- CVE-2022-29862
- CVE-2022-29864

Changes in Firmware 2022.0.8
Includes all firmware 2022.0.7 fixes

Curl

– CVE-2022-22576
– CVE-2022-27778
– CVE-2022-27779
– CVE-2022-27782
– CVE-2022-27774
– CVE-2022-27776
– CVE-2022-30115
– CVE-2022-27780
– CVE-2022-27781
– CVE-2022-27775
– CVE-2022-32207
– CVE-2022-32206
– CVE-2022-32208
– CVE-2022-32205

Cyrus SASL

– CVE-2019-19906
– CVE-2022-24407

Vim

– CVE-2022-1154
– CVE-2022-0943
– CVE-2022-1160
– CVE-2022-1381
– CVE-2022-0729
– CVE-2022-0572
– CVE-2022-1420
– CVE-2022-0696
– CVE-2022-0685
– CVE-2022-0714
– CVE-2022-0361
– CVE-2022-0368
– CVE-2021-3973
– CVE-2021-3796
– CVE-2021-4166
– CVE-2022-1733
– CVE-2022-1796
– CVE-2022-1621
– CVE-2022-1616
– CVE-2022-1619
– CVE-2022-1629
– CVE-2022-1735
– CVE-2022-1769
– CVE-2022-1785
– CVE-2022-1620
– CVE-2022-1674
– CVE-2022-1771
– CVE-2022-1886
– CVE-2022-1851
– CVE-2022-1898
– CVE-2022-1927
– CVE-2022-1942
– CVE-2022-1720
– CVE-2022-2129
– CVE-2022-2175
– CVE-2022-2182
– CVE-2022-2183
– CVE-2022-2343
– CVE-2022-2207
– CVE-2022-2210
– CVE-2022-2344
– CVE-2022-2304
– CVE-2022-2345
– CVE-2022-2208
– CVE-2022-2231
– CVE-2022-2287
– CVE-2022-2285
– CVE-2022-2284
– CVE-2022-2286
– CVE-2022-2289
– CVE-2022-2288
– CVE-2022-2264
– CVE-2022-2206
– CVE-2022-2257

Changes in Firmware 2022.0.3
BPC 9102S only

OPC UA

– CVE-2021-45117