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

14 February 2023
2023/00001

Security Advisory: Multiple Linux component vulnerabilities fixed in latest PLCnext Firmware release 2023.0.0 LTS

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0

Advisory Title

Update for PLCnext Firmware releases based on actual vulnerability reports for Linux components and further security enhancements.

Advisory ID

VDE-2023-001

Vulnerability Description

PLCnext Control AXC F x152 and RFC 4072S 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. All PLCnext Control targets are updated regularly with new LTS versions no matter if they are certified or not.

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

...

Affected products

Article no	Article	Affected versions	Build number	Fixed Version
1151412	AXC F 1152	< 2023.0.0 LTS	< 23.0.0.41	Download
2404267	AXC F 2152	< 2023.0.0 LTS	< 23.0.0.65	Download
1069208	AXC F 3152	< 2023.0.x LTS	Please check product webpage	Download
1051328	RFC 4072S	< 2023.0.x LTS	Please check product webpage	Download
1246285	BPC 9102S	< 2023.0.x LTS	Please check product webpage	Download
1136419	RFC 4072R	< 2023.0.x LTS	Please check product webpage	Download
1264327	ENERGY AXC PU	<= V04.15.00.01	Please check product webpage	V04.16.00.00

The firmware version 2023.0.x LTS will be made available successively for the devices listed above by the end of Q1/2023. Please check the respective product website.

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-2023-001

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 2023.0.0 LTS Firmware Release. PHOENIX CONTACT recommends to always use an up-to-date version of the PLCnext Engineer.

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 (2023-02-14): Initial publication

Annex 1: Fixed Vulnerabilities

Changes in Firmware 2023.0.0 LTS

Busybox

– CVE-2022-30065

Curl

– CVE-2022-32207
– CVE-2022-32206
– CVE-2022-32208
– CVE-2022-32205
– CVE-2022-35252
– CVE-2022-42915
– CVE-2022-42916

Dpkg

– CVE-2022-1664

E2fsprogs

– CVE-2022-1304

Git

– CVE-2022-29187
– CVE-2022-39260
– CVE-2022-39253

Gnutls

– CVE-2022-2509

Libtirpc

– CVE-2021-46828

Libxml2

– CVE-2022-40304

Libexpat

– CVE-2022-40674
– CVE-2022-43680

Linux

– CVE-2022-1015
– CVE-2022-1016

Logrotate

– CVE-2022-1348

OpenSSL

– CVE-2022-2097

Python

– CVE-2022-42919

SSH

– CVE 2002-20001
The following vulnerable DHE KEY algorithm(s) of the openSSH server have been completely removed:
– diffie-hellman-group14-sha256
– diffie-hellman-group16-sha512
– diffie-hellman-group18-sha512
– diffie-hellman-group-exchange-sha256

StrongSwan

– CVE-2022-40617

Sudo

– CVE-2022-43995

Vim

– CVE-2022-1927
– CVE-2022-1942
– 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-2022-2231
– CVE-2022-2287
– CVE-2022-2284
– CVE-2022-2289
– CVE-2022-2288
– CVE-2022-2264
– CVE-2022-2206
– CVE-2022-2257
– CVE-2022-2208
– CVE-2022-2285
– CVE-2022-2286
– CVE-2022-2522
– CVE-2022-2571
– CVE-2022-2580
– CVE-2022-2581
– CVE-2022-2598
– CVE-2022-3234
– CVE-2022-3235
– CVE-2022-3256
– CVE-2022-3278
– CVE-2022-3296
– CVE-2022-3297
– CVE-2022-3324

– CVE-2022-3352
– CVE-2022-3705

Zlib

– CVE-2022-37434

HMI

– Hardening against DoS attacks.
– Hardening against memory leak problems in case of network attacks.

WBM

– Umlauts in the password of the “User Manager” were not handled correctly.
The password rule for upper and lower case was not followed. This could lead to unintentionally weaker passwords.

– Hardening of WBM against Cross-Site-Scripting.

User Manager

– In security notifications “SecurityToken” was always displayed as “0000000” when creating or modifying users.

– Hardening of Trust and Identity Stores.