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 March 2023
2023/00003

Security Advisory for ENERGY AXC PU

Publication Date: 2023-03-14
Last Update: 2023-03-14
Current Version: V1.0

Advisory Title

Multiple vulnerabilities have been discovered in CODESYS Control V3 runtime system utilized by ENERGY AXC PU.

Advisory ID

VDE-2023-003

Vulnerability Description

Multiple vulnerabilities have been discovered in CODESYS Control V3 runtime system.
For details regarding the single vulnerabilities please refer to the security advisories issued by CODESYS.

CODESYS Security Advisory 2022-02
CODESYS Security Advisory 2022-04
CODESYS Security Advisory 2022-06
CODESYS Security Advisory 2022-09

...

Affected products

Article no	Article	Affected versions	Fixed version
1264327	ENERGY AXC PU	< V04.15.00.00	>= V04.15.00.00

Impact

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. Such products contain communication servers for the CODESYS protocol to enable communication with clients. These servers contain following vulnerabilities:

CVE-2022-22513:
An authenticated remote attacker can cause a null pointer dereference in the CmpSettings component of the affected CODESYS products which leads to a crash.

CVE-2022-22514:
An authenticated, remote attacker can gain access to a dereferenced pointer contained in a request. The accesses can subsequently lead to local overwriting of memory in the CmpTraceMgr, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.

CVE-2022-22515:
A remote, authenticated attacker could utilize the control program of the CODESYS Control runtime system to use the vulnerability to read and modify the configuration file(s) of the affected products.

CVE-2022-22517:
An unauthenticated, remote attacker can disrupt existing communication channels between CODESYS products by guessing a valid channel ID and injecting packets. This results in the communication channel to be closed.

CVE-2022-30792:
In CmpChannelServer of CODESYS V3 in multiple versions an uncontrolled resource consumption allows an unauthorized attacker to block new communication channel connections. Existing connections are not affected.

Classification of Vulnerability

CVE-2022-22513
Base Score: 6.5
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-476

...

CVE-2022-22514
Base Score: 7.1
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
CWE: CWE-119

CVE-2022-22515
Base Score: 8.1
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
CWE: CWE-668

CVE-2022-22517
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-330

CVE-2022-30792
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE: CWE-400

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

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.

Acknowledgement

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

History

V1.0 (2023-03-14): Initial publication