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

100 years of passion for technology and innovation

12 December 2023
2023/00013-4

Security Advisory for PLCnext Control. “Insufficient Read and Write Protection to Logic and Runtime Data”

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0

Advisory Title

PLCnext Control provides insufficient read and write protection to logic and runtime data.

Advisory ID

CVE-2023-46142
VDE-2023-056

Vulnerability Description

PLCnext Control provides authentication and integrity check for the application.
An authenticated, skilled attacker might be able to manipulate the application (e.g.: logic files, executable logic, configurations) in a special crafted way that the integrity check will not be able to recognize these tampering attempts which are then difficult to remove.

To successfully exploit this vulnerability, the attacker must have access to the application either with PLCnext Engineer on the Engineering station, the stored application, the application during download or the application storage on the PLC.

Affected products

PLCnext Control:

Article	Article number	Version
AXC F 1152	1151412	<= 2024.0
AXC F 2152	2404267	<= 2024.0
AXC F 3152	1069208	<= 2024.0
RFC 4072S	1051328	<= 2024.0
BPC 9102S	1246285	<= 2024.0
RFC 4072R	1136419	<= 2024.0
EPC 1502	1185416	<= 2024.0
EPC 1522	1185423	<= 2024.0

PLCnext Engineer:

Article	Article number	Version
PLCnext Engineer	1046008	<= 2024.0

Impact

The identified vulnerabilities allow attackers to generate logic files or upload logic with arbitrary malicious code to PLCnext Control once they have access to the engineering station running PLCnext Engineer or can communicate with the controllers.
Attackers must have authenticated network or physical access to the engineering station or controller to exploit this vulnerability.

Classification of Vulnerability

CVE-2023-46142
Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE-732: Incorrect Permission Assignment for Critical Resource

Temporary Fix / Mitigation

PLCnext Control is developed and designed for use in protected industrial networks. In this approach, the production plant is protected against attacks, especially from the outside, by a multi-level perimeter, including firewalls, and by dividing the plant into OT zones using firewalls.

This concept is supported by organizational measures in the production facility as part of a security management system. To achieve security, measures are required at all levels. It must be ensured that the application is always transferred or stored in protected environments.

This applies to both data in transmission and data at rest. Connections between the engineering tools (PLCnext Engineer) and PLCnext Control must always be in a locally protected environment or, in the case of remote access, protected by VPN.

Project data should not be sent as a file via email or other transmission mechanisms without additional integrity and authenticity checks. Project data should only be stored in protected environments.

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note:
Application note Security

PLCnext Control provides a feature set that supports users in setting up a separated protected environment, for example, by using separated Ethernet ports, firewalls, user and certificate management and integrity checks. These features can reduce the attack surface of this vulnerability.

For more information's refer to the PLCnext Info Centers:
PLCnext Info Center
PLCnext Security Info Center

Concepts how to use PLCnext Control to establish protected industrial networks are described in the Security Context description Generic security concept (plcnext.help).

Remediation

PLCnext Control security feature set and hardening are continuously improved.
Please check the PLCnext Control product download pages for updated versions and the PSIRT webpage https://phoenixcontact.com/psirt for updated information's and firmware regularly.

We recommend that our customers always use the latest LTS versions, as known security vulnerabilities are regularly fixed. The latest version at the time of publication of this advisory is 2023.0.7 LTS Hotfix.

Acknowledgement

This vulnerability was reported by Reid Wightman of Dragos, Inc.
Phoenix Contact would like to thank Dragos for the cooperation and detailed communication to prepare this coordinated disclosure.

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

History

V1.0 (2023-12-12): Initial publication