Phoenix Contact Inc.
P.O. BOX 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300

Product Change Notification

PCN-AS-9333-2023

Business Unit	Product Line Code	Type of Change	Action	Date of Issue
AS - Automation Systems	DRA	Product Change Notification	Notify Distributors and Field	12/18/2023

The following Phoenix Contact products have been modified. Existing specifications will be met or exceeded. Please review and acknowledge this document and inform your personnel as needed.

Product Change Notification

Description for Product Change Notification

Advisory ID

CVE-2023-46144
VDE-2023-058

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 .

PLCnext Engineer warns users if the PLC logic is different from the current loaded project when Online mode is activated . In addition, during loading an application on the PLC, a Project Integrity Warning logging entry is generated . A skilled attacker might be able to manipulate the application in a special crafted way that the integrity check will not be able to recognize tampering attempts.

Affected products

All products listed below for firmware Version 2024.0 and earlier

Impact

The identified vulnerabilities allow to download and execute manipulated applications on PLCnext Control. Potential tampered applications might not be discovered

Classification of Vulnerability

CVE-2023-46144
Base Score: 7.7
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N CWE-494: Download of Code Without Integrity Check

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:

Product Change Notification

https://dam-mdc.phoenixcontact.com/asset/156443151564/
0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

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 - Home (plcnext.help)
PLCnext Security Info Center -Home (plcnext.help)

PLCnext Control provides project data integrity checks, information's about the default configuration are provided in the topic Checking project data integrity (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

Stock Status	
Can existing stock still be used?	
Is mixture of stock acceptable?	

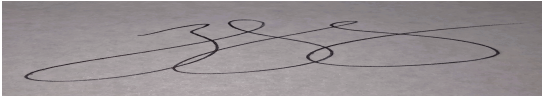| Transaction Dates	
Date modification goes into effect from Germany:	12/12/2023
Expected first shipment (from Phoenix Contact) of the modified products(s):	12/12/2023

Product Change Notification

Should you have any issues with the timeline or content of this product change, please contact Phoenix Contact using the information below. Customers should acknowledge receipt of the PCN within 30 days of delivery of the PCN; provided, however, that the failure to acknowledge receipt does not affect the product change or the effective date thereof.

Contact Info:
Ted Thayer
tthayer@phoenixcontact.com

Thank you,

Zachary Stank

Product Marketing Manager

Product Change Notification

Part #	Type Description
1151412	AXC F 1152
2404267	AXC F 2152
1069208	AXC F 3152
1051328	RFC 4072S
1136419	RFC 4072R
1185416	EPC 1502
1185423	EPC 1522
1246285	BPC 9102S
1046008	PLCNEXT ENGINEER