PHOENIX CONTACT
INSPIRING INNOVATIONS

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

Product Change Notification

PCN-AS-8007-2022

Business Unit	Product Line Code	Type of Change	Action	Date of Issue
AS - Automation Systems	DRA	Product Change Notification	Notify Distributors and Field	6/27/2022

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

ProConOS/ProConOS eCLR designed for use in closed industrial networks providing insufficient logic controls allowing attackers to upload logic with arbitrary malicious code.

Advisory ID

CVE-2022-31801
VDE-2022-026

Vulnerability Description

Increased Security attacks in the OT arena and research of Forescout makes it necessary to publish this advisory giving users hints according to basic security measures to support automation systems using existing devices based on ProConOs/ProConOS eCLR.

ProConOs/ProConOS eCLR. controller runtime system has been offered as a Software Development Kit (SDK) to automation suppliers that build their own automation devices. ProConOs/ProConOS eCLR. is embedded into automation suppliers' hardware, real-time operating systems (RTOS), firmware, and I/O systems. The logic had been designed without integrity and authenticity checks which was state of the art when developing the products.

Affected products

Article	Article number
ProConOS	All variants and versions
ProConOS eCLR	All variants and versions
MULTIPROG	All variants and versions

Impact

The identified vulnerability allows attackers uploading logic with arbitrary malicious code once having access to the communication to products that are utilizing ProConOs/ProConOS eCLR. Attackers must have network or physical controller access to exploit this vulnerability. This vulnerability affects all versions of ProConOs/ProConOS eCLR.. and MULTIPROG from Phoenix Contact Software (formerly KW-Software).

Classification of Vulnerability

CVE-2022-31801
Base Score: 9.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE-345: Insufficient Verification of Data Authenticity

Temporary Fix / Mitigation

Industrial controllers based on ProConOs/ProConOS eCLR. are typically developed and designed for the use in closed industrial networks using a defense-in-depth approach focusing on Network segmentation. In such approach, the production plant is protected against attacks, especially from the outside, by a multi-level perimeter, including firewalls as well as dividing the plant into OT zones by using firewalls. This concept is supported by organizational measures in the production plant as part of a security management system. To accomplish security here measures are required at all levels.

Manufacturers using ProConOs/ProConOS eCLR. in their automation devices are advised to check their implementation and may publish an advisory according to their product.

Users of automation devices utilizing ProConOs/ProConOS eCLR. in their automation systems may check if their

Product Change Notification

application requires additional security measures like an adequate defense– in-depth networking architecture, the use of virtual private networks (VPNs) for remote access, as well as the use of firewalls for network segmentation or controller isolation.

Users should check their manufacturers security advisories for more adequate information according to their dedicated device.

Generic information and recommendations for security measures to protect network-capable devices can be found in the application note:
Application note Security

Acknowledgement

This vulnerability was reported by Forescout.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder .
PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

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

Transaction Dates	
Date modification goes into effect from Germany:	6/27/2022
Expected first shipment (from Phoenix Contact) of the modified products(s):	6/27/2022

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
2700973	ILC 131 ETH
2700974	ILC 151 ETH
2700975	ILC 171 ETH 2TX
2700976	ILC 191 ETH 2TX
2700988	AXC 1050
2700989	AXC 3050
2701295	AXC 1050 XC