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

21 June 2022
300550605

# Security Advisory for logic without integrity check in ProConOS/ProConOS eCLR SDK and MULTIPROG Engineering tool

## Advisory Title

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 aera 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.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

## 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 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.

Users should ensure that the logic is always transferred or stored in protected environments. This is valid for data in transmission as well as data in rest. Connections between the Engineering Tools and the controller must always be in a locally protected environment or protected by VPN for remote access. Project data shouldn’t send as a file via e-mail or other transfer mechanisms without additional integrity and authenticity checks.
Project data should save in protected environments only.

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.