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 unauthenticated Protocols in ProConOS/ProConOS eCLR SDK and MULTIPROG Engineering tool

Advisory Title

ProConOS/ProConOS eCLR designed for use in closed industrial networks provide communication protocols without authentication.

Re-publication. Please also refer the original ICS-CERT advisory ICSA-15-013-03 published 13 January 2015.

Advisory ID

CVE-2014-9195
VDE-2022-028

Vulnerability Description

ProConOS/ProConOS eCLR PLC 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 communication layer had been designed without authentication for easy integration intentionally but offered the option to be embedded into authentication mechanisms and security layers of automation suppliers.

...

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 for unauthenticated users to modify programs in some controllers that are utilizing ProConOS/ProConOS eCLR and MULTIPROG products. Attackers who reengineer the communication protocols and have network or physical controller access can 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-2014-9195
Base Score: 9.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE-306: Missing Authentication for Critical Function

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.

...

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 Reid Wightman of Digital Bond and re-discovered 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.