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
2023/00013-2

Security Advisory for MULTIPROG Engineering tool and ProConOS eCLR SDK. „Integrity check fails to identify out-of-band logic changes“

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

Advisory Title

ProConOS eCLR integrity check fails to identify out-of-band logic changes.

Advisory ID

CVE-2023-5592
VDE-2023-054

Vulnerability Description

Increased Security attacks against OT infrastructure and research of Dragos 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 application (e.g.: logic files, executable logic, configurations) had been designed without integrity and authenticity check which was state of the art when developing the products.

A CRC Check waring the user if the application of the Engineering tool and the PLC differs can be manipulated.

Users need to check with their device vendors if they are affected by this attack vulnerability or if the specific device integration mitigates this attack vector.

Affected products

Article	Article number
ProConOS eCLR (SDK)	All variants and versions
MULTIPROG	All variants and versions

Impact

The identified vulnerability allows to download and execute applications without integrity checks. Potential tampered application might not be discovered.
This vulnerability affects all versions of ProConOS eCLR and MULTIPROG from Phoenix Contact (formerly KW-Software).

Classification of Vulnerability

CVE-2023-5592
Base Score: 8.6
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:S/C:N/I:H/A:N
CWE-494: Download of Code Without Integrity Check

Temporary Fix / Mitigation

Industrial controllers based on ProConOS eCLR runtime are typically designed for use in closed industrial networks with a defense-in-depth approach focusing on network segmentation. In such

...

an approach, the production facility is protected from attacks, especially from the outside, by a multi-level perimeter including firewalls as well as the division of the facility into OT zones using firewalls. This concept is supported by organizational measures in the production plant as part of a security management system. To achieve security here, measures are required at all levels. Engineering stations using MULTIPROG must also be part of closed industrial networks.

Manufacturers who use ProConOS eCLR runtime in their automation devices are recommended to review their implementation and, if necessary, publish corresponding advisories for their products.

Users of automation devices that use MULTIPROG Engineering and ProConOS eCLR runtime in their automation systems must check whether their application requires additional security measures. These include, for example, adequate defense-in-depth network architecture, the use of virtual private networks (VPNs) for remote access, and the use of firewalls for network segmentation or controller isolation. Users should review their manufacturer's security advisories for more appropriate information about their specific device.

Users should ensure that logic is always transmitted or stored in protected environments.
This applies both to data in transmission and to data at rest. Connections between engineering tools and the controller must always be protected in a locally protected environment or via VPN for remote access. 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

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