PROFIBUS Nutzerorganisation e.V. (PNO)
A member of PI (PROFIBUS & PROFINET International)
security@profinet.com
https://www.profibus.com/pi-organization/cyber-security-incident-response-team

PROFINET Security Advisory

Title of the advisory: Improper Access Control for DCP Services

PNO Identifier: PISA-001

CVE Identifier (if assigned): **-**
CVSS v3.1 vector: **CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H**
CVSS v3.1 Base Score: **6.5**

Overview about the vulnerability

PI Organization has been informed about a behavior of PROFINET products which under certain circumstances can lead to a permanent loss of communication capability between PROFINET Controller and PROFINET Device in case an adversary with direct (physical) access to the PROFINET network attacks the devices by using DCP services of the PROFINET protocol.

The reason for this lies in the nature of the DCP service provided by the PROFINET protocol. This DCP service can be used to change or reset device parameters via DCP command. Examples are DCP-Set (NameOfStation) or DCP-Set (Reset-to-Factory).

The PROFINET specification used to build the reported device was an older version that did not include any security functions to prevent this behavior. Newer versions of the specification address this issue by introducing the Security Class 1 [3].

Under certain conditions, an attacker – with direct access to the OT network – can prevent the PROFINET Controller from establishing communication with a PROFINET Device. Manual intervention by the user is required.

Affected Products:

All PROFINET products that do not comply to the PROFINET Security Class 1. If this feature is used by an attacker with direct (physical) access to the PROFINET network, communication between controller and device can be disrupted under certain circumstances. It cannot be ensured under all circumstances that the PROFINET device can be put back into operation without human user intervention.

Impact of the vulnerability

- The attack causes a temporary interruption of the communication, until the device name is set to the correct value.

CVSS V3.1 Score:

CVSS v3.1 Base Score	6.5

CVSS v3.1

AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C/CR:X/IR:X/AR:H/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:X/MI:X/MA:H

CWE

CWE-862: Missing Authorization
CWE-1314: Missing Write Protection for Parametric Data Values

Fixing of the vulnerability

PROFIBUS and PROFINET International (PI) is in the process to upgrade the PROFINET protocol specification with security features. An updated version of the PROFINET-Specification Version 2.4 MU4 [1][2][5] is available. This updated version provides the necessary security measures to mitigate the vulnerability.

Independent of the PROFINET Security Class 1, PI recommends that all users plan PROFINET systems in accordance with the PROFINET Security Guideline [4] in order to establish a defense in depth approach and in order to separate the OT network from the IT network.

References

[1] PROFIBUS Nutzerorganisation e.V.: Application Layer protocol for decentralized periphery, Technical Specification for PROFINET. Version 2.4 MU4. May 2023 URL: https://www.profibus.com/download/profinet-specification.

[2] PROFIBUS Nutzerorganisation e.V.: Application Layer services for decentralized periphery, Technical Specification for PROFINET. Version 2.4 MU4 – May. 2023. URL: https://de.profibus.com/downloads/profinet-specification/.

[3] PROFIBUS Nutzerorganisation e.V.: Security Class 1 for PROFINET-Security. URL: https://www.profibus.com/download/profinet-security-guideline.

[4] PROFIBUS Nutzerorganisation e.V.: PROFINET Security Guideline. Order No..: 7.002. 2013. URL: https://www.profibus.com/download/profinet-security-guideline/.

[5] PROFIBUS Nutzerorganisation e.V.: GSDML - Technical Specification for PROFINET. Order No.: 2.352. 2023. URL: https://www.profibus.com/download/gsdml-gsdx-specification-for-profinet.

Affected Protocol versions / affected protocol stacks /affected products

All products that do not adhere to the PROFINET Security Class 1. Note: Devices supporting the Security Classes 1 must have DCP Set disabled.

All Protocol versions prior to PROFINET Version 2.4 MU4.

Acknowledgement

Terms of use

PI produced this advisory with the expected care. However, PI makes no warranty of any kind, express or implied, as to the accuracy of vulnerability reports and their resolution, including but not limited to any warranty of title, implied warranty or warranty of fitness for a particular purpose or use.

In no event shall PI be liable for any errors contained herein or for any indirect, incidental, special, consequential, trust or coverage damages, including loss of profits, revenue, data or use, suffered by any user or third party.