TLP:WHITE

VDE-2025-029: Phoenix Contact: Security Advisory for AXL F BK and IL BK bus couplers

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue May 13 13:00:00 CEST 2025	Engine: 2.5.23
Current release date: Tue May 13 13:00:00 CEST 2025	Build Date: Thu Apr 24 16:15:28 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 7.5	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2025-029, PCSA-2025/00006	

Summary

A denial of service (DoS) attack targeting port 80 (http service) can overload the device (CWE-770). This behaviour has been observed when running network security scanners.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

Impact

A successful attack leads to an overload of the device and the hardware watchdog is triggered. Process data behaves according to the configured substitute value behavior.

The bus coupler requires a manual restart (resetting the power supply, pressing the reset button or executing the SNMP reset command) to reestablish communication within the Industrial Ethernet (e.g. PROFINET IO, Modbus/TCP, EtherNet/IP).

Mitigation

Affected bus couplers are designed and developed for the use in closed industrial networks. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

If the use of scanners is mandatory for network security in closed production networks, it is recommended to exclude or disable denial of service tests that target port 80. Most network scanners offer options to individually disable certain tests or to apply exclusions by clustering device types and test categorization functions.

Remediation

To further improve security, fixed firmware versions are available for the items listed in the "Fixed" section. A fix for products marked as "discontinued" is not planned. All other listed products will receive a bugfix at the next revision.

Product description

Bus coupler for Axioline F and Inline Remote-I/O-system

Product groups

Affected Products

- Firmware <= 1.33 installed on AXL F BK PN TPS
- Firmware <= 1.33 installed on AXL F BK PN TPS XC
- Firmware <= 1.06 installed on AXL F BK PN (discontinued)
- Firmware <= 1.06 installed on AXL F BK PN XC (discontinued)
- Firmware <= 1.35 installed on AXL F BK SAS (discontinued)
- Firmware <= 1.31 installed on AXL F BK ETH
- Firmware <= 1.31 installed on AXL F BK ETH XC
- Firmware <= 1.30 installed on AXL F BK EIP
- Firmware <= 1.30 installed on AXL F BK EIP EF
- Firmware <= 1.30 installed on AXL F BK EIP XC
- Firmware <= 1.13 installed on IL PN BK-PAC
- Firmware <= 1.00 installed on IL ETH BK-PAC
- Firmware <= 1.42 installed on IL ETH BK DI8 DO4 2TX-PAC
- Firmware <= 1.12 installed on IL EIP BK DI8 DO4 2TX-PAC

Fixed

- Firmware 2.00 installed on AXL F BK PN TPS (available Q4/2025)
- Firmware 2.00 installed on AXL F BK PN TPS XC (available Q4/2025)
- Firmware 1.32 installed on AXL F BK ETH
- Firmware 1.32 installed on AXL F BK ETH XC

Vulnerabilities

CVE-2025-2813

Summary

An unauthenticated remote attacker can cause a Denial of Service by sending a large number of requests to the http service on port 80.

CWE:	CWE-770: Allocation of Resources Without Limits or Throttling
Release date:	Tue May 13 13:00:00 CEST 2025

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <= 1.33 installed on AXL F BK PN TPS Order number: 2403869	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.33 installed on AXL F BK PN TPS XC Order number: 1068857	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.06 installed on AXL F BK PN (discontinued) Order number: 2701815	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.06 installed on AXL F BK PN XC (discontinued) Order number: 2701222	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.35 installed on AXL F BK SAS (discontinued) Order number: 2701457	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.31 installed on AXL F BK ETH Order number: 2688459	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.31 installed on AXL F BK ETH XC Order number: 2701949	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.30 installed on AXL F BK EIP Order number: 2688394	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.30 installed on AXL F BK EIP EF Order number: 2702782	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.30 installed on AXL F BK EIP XC Order number: 1167192	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.13 installed on IL PN BK-PAC Order number: 2403696	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.00 installed on IL ETH BK-PAC Order number: 2702372	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.42 installed on IL ETH BK DI8 DO4 2TX-PAC Order number: 2703981	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Firmware <= 1.12 installed on IL EIP BK DI8 DO4 2TX-PAC Order number: 2897758	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Fixed

Product
Firmware 2.00 installed on AXL F BK PN TPS (available Q4/2025) Order number: 2403869 (Download)
Firmware 2.00 installed on AXL F BK PN TPS XC (available Q4/2025) Order number: 1068857 (Download)
Firmware 1.32 installed on AXL F BK ETH Order number: 2688459 (Download)
Firmware 1.32 installed on AXL F BK ETH XC Order number: 2701949 (Download)

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for Coordination (see: https://certvde.com/en/)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- VDE-2025-029: Phoenix Contact: Security Advisory for AXL F BK and IL BK bus couplers - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-029/
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- PCSA-2025/00006 (EXTERNAL): https://phoenixcontact.com/psirt
- VDE-2025-029: Phoenix Contact: Security Advisory for AXL F BK and IL BK bus couplers - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-029.json

Revision history

Version	Date of the revision	Summary of the revision
1	Tue May 13 13:00:00 CEST 2025	Initial revision

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/