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

07 June 2021
300463994

Security Advisory for AXL F BK and IL BK products

Advisory Title

Undocumented password protected FTP access in certain devices of the AXL F BK and IL BK product families.

Advisory ID

CVE-2021-33540
VDE-2021-021

Vulnerability Description

An undocumented password protected FTP access to the root directory exists in certain devices of the AXL F BK and IL BK product families (CWE-798).

Affected products

Article no	Article	Affected revisions
1068857	AXL F BK PN TPS XC	FW < 1.30, HW < 01
2403869	AXL F BK PN TPS	FW < 1.30, HW < 02
2688394	AXL F BK EIP	FW < 1.30, HW < 05
2702782	AXL F BK EIP EF	FW < 1.30, HW < 01
2688459	AXL F BK ETH	FW < 1.30, HW < 05
2701949	AXL F BK ETH XC	FW < 1.30, HW < 05
2701686	AXL F BK S3	FW < 1.40, HW < 05
2701815	AXL F BK PN	all revisions
2701222	AXL F BK PN XC	all revisions
2702177	AXL F BK ETH NET2	all revisions
2701457	AXL F BK SAS	all revisions

2403696	IL PN BK-PAC	all revisions
2703994	IL PN BK DI8 DO4 2TX-PAC	all revisions
2878379	IL PN BK DI8 DO4 2SCRJ-PAC	all revisions
2701388	IL ETH BK DI8 DO4 2TX-XC-PAC	all revisions
2703981	IL ETH BK DI8 DO4 2TX-PAC	all revisions
2897758	IL EIP BK DI8 DO4 2TX-PAC	all revisions
2692380	IL S3 BK DI8 DO4 2TX-PAC	all revisions

Articles not listed above are not affected.

Impact

An attacker who was able to obtain the hard-coded password to FTP access could access the FTP area and read the scrambled monitoring information of the device.

Classification of Vulnerability

Base Score: 7.3
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Temporary Fix / Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Remediation

For the following devices a firmware update is available that disabled the above-mentioned undocumented FTP access. PHOENIX CONTACT recommends upgrading these devices to the latest firmware.

Article no	Article	Affected versions	FW Download
1068857	AXL F BK PN TPS XC	FW ≥ 1.30, HW 01	Link
2403869	AXL F BK PN TPS	FW ≥ 1.30, HW 02	Link
2688394	AXL F BK EIP	FW ≥ 1.30, HW 05	Link
2702782	AXL F BK EIP EF	FW ≥ 1.30, HW 01	Link
2688459	AXL F BK ETH	FW ≥ 1.30, HW 05	Link
2701949	AXL F BK ETH XC	FW ≥ 1.30, HW 05	Link
2701686	AXL F BK S3	FW ≥ 1.40, HW 05	End Q4 2021

...

Acknowledgement

This vulnerability was discovered by Secuvera.

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.