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

18 September 2018
300410216/pbsa56

Security Advisory for Phoenix Contact AXL F BK

Advisory Title

Denial of Service due to incorrect handling of web request

Advisory ID

VDE-2018-015
CVE-2018-16994

Vulnerability Description

Incorrect handling request with non-standard symbols allows remote attackers to initiate a complete lock up of the bus coupler. Authentication of the request is not required.

Affected products

Article	Article number	Affected Firmware versions
AXL F BK PN	2701815	up to and including 1.0.4
AXL F BK ETH	2688459	up to and including 1.12
AXL F BK ETH XC	2701949	up to and including 1.11

Impact

The device stops responding to any network or local port, consequently shutting down this part of the automation system. The bus coupler needs to be restarted by disconnecting the power supply.

Classification of Vulnerability

Base Score: 7.5
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

...

Mitigation

Customers using affected Phoenix Contact AXL F BK are recommended to operate the devices in closed networks or protected with a suitable firewall.
For detailed information on our recommendations for measures to protect network-cabable devices, please refer to our application note:

https://www.phoenixcontact.com/assets/downloads_ed/local_pc/web_dwl_technical_info/ah_en_industrial_security_107913_en_01.pdf

Acknowledgement

This vulnerability was reported by Anne Borcherding, Steffen Pfrang, David Meier und Christian Haas from Fraunhofer IOSB