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

11 May 2018
300405373/pbsa56

# Security Advisory for FL SWITCH 3xxx, FL SWITCH 4xxx, FL SWITCH 48xx products [CVE-2018-10730]

## Advisory Title

Authenticated Remote Code Execution.

## Advisory ID

CVE-2018-10730
VDE-2018-004

## Vulnerability Description

An attacker with permission to transfer configuration files to/from the switch or permission to upgrade firmware, is able to execute arbitrary OS shell commands. CGI applications config_transfer.cgi and software_update.cgi are prone to OS command injection through targeted manipulation of their web-request headers.

## Affected products

All Phoenix Contact managed FL SWITCH 3xxx, 4xxx, 48xx products running firmware version 1.0 to 1.33

## Impact

If the vulnerability is exploited, the attacker may create their own executable files that could further exploit the integrity of the managed FL SWITCH.  For example, the attacker may deny switch network access.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Executive Vice Presidents:
Frank Stührenberg (CEO)
Roland Bent
Prof. Dr. Gunther Olesch
Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

## Classification of Vulnerability

Base Score: 9.1 (Critical)
Vector: CVSS: 3.0 /AV:N /AC:L /PR:H /UI:N /S:C /C:H /I:H /A:H

## Temporary Fix / Mitigation

Customers using Phoenix Contact managed FL SWITCH devices with affected firmware versions are recommended to disable the switch Web Agent.

## Remediation

Customers using Phoenix Contact managed FL SWITCH devices with affected firmware versions are recommended to update the firmware to version 1.34 or higher which fixes this vulnerability. The updated firmware may be downloaded from the managed switch product page on the Phoenix Contact website.

## Acknowledgement

This vulnerability was discovered by Vyacheslav Moskvin (Positive Technologies).