

11 May 2018
300405373/pbsa56

Security Advisory for FL SWITCH 3xxx, FL SWITCH 4xxx, FL SWITCH 48xx products [CVE-2018-10728]

Advisory Title

Stack-based Buffer Overflow due to improper length check in *cookies_get_value* function.

Advisory ID

CVE-2018-10728
VDE-2018-006

Vulnerability Description

An attacker may insert a carefully crafted cookie into a GET menu_pxc.cgi or GET index.cgi request to cause a buffer overflow that can initiate a Denial of Service attack and execute arbitrary code.

Affected products

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

Impact

If vulnerability is exploited, the attacker may disable Web and Telnet services and execute arbitrary code.

Classification of Vulnerability

Base Score: 8.1(High)
Vector: CVSS: 3.0 /AV:N /AC:H /PR:N /UI:N /S:U /C:H /I:H /A:H

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: DEUTDE33XXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADE33XXX
IBAN:
DE31 4764 0051 0226 0396 00

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 Evgeniy Druzhinin, Georgy Zaytsev, and Ilya Karpov (Positive Technologies).