PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

07 June 2021
300505868

Security Advisory for FL SWITCH SMCS series

Advisory Title

Multiple vulnerabilities have been discovered in the current firmware of the PHOENIX CONTACT FL SWITCH SMCS series switches.

Advisory ID

CVE-2021- 20003
CVE-2021- 20004
CVE-2021- 20005
VDE-2021-023

Vulnerability Description

TCP-Fragmentation DoS vulnerability (CVE-2021- 20003, CWE-404):
Fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP-, and ICMP Echo-service. The switching functionality of the device is not affected.

LLDP XSS vulnerability (CVE-2021- 20004, CWE-79):
An attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client.

Urgent-Flag DoS vulnerability (CVE-2021- 20005, CWE-362):
If an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards.

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

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, 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

...

Affected products

Article no	Article	Affected versions
2700996	FL SWITCH SMCS 16TX	<= 4.70
2700997	FL SWITCH SMCS 14TX/2FX	<= 4.70
2701466	FL SWITCH SMCS 14TX/2FX-SM	<= 4.70
2891123	FL SWITCH SMCS 8GT	<= 4.70
2891479	FL SWITCH SMCS 6GT/2SFP	<= 4.70
2989103	FL SWITCH SMCS 8TX-PN	<= 4.70
2989093	FL SWITCH SMCS 4TX-PN	<= 4.70
2989226	FL SWITCH SMCS 8TX	<= 4.70
2989323	FL SWITCH SMCS 6TX/2SFP	<= 4.70
2700290	FL SWITCH SMN 6TX/2POF-PN	<= 4.70
2989501	FL SWITCH SMN 8TX-PN	<= 4.70
2989543	FL SWITCH SMN 6TX/2FX	<= 4.70
2989556	FL SWITCH SMN 6TX/2FX SM	<= 4.70
2989365	FL NAT SMN 8TX	<= 4.63
2702443	FL NAT SMN 8TX-M	<= 4.63

Impact

An attacker may use the vulnerabilities described above to provoke a denial of service to defeat certain management functions of the device or use the XSS vulnerability to attack the client PC.

Classification of Vulnerability

TCP-Fragmentation DoS vulnerability (CVE-2021- 20003):
Base Score: 5.3
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

LLDP XSS vulnerability (CVE-2021- 20004):
Base Score: 7.4
Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N

Urgent-Flag DoS vulnerability (CVE-2021- 20005):
Base Score: 7.5
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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

...

Acknowledgement

These vulnerabilities have been discovered and reported by Anne Borcherding, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB.

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.