

25 January 2022
300537202

Security Advisory for FL SWITCH 2xxx series

Advisory Title

An unprivileged user connected via SSH Command Line Interface (CLI) gains admin privileges.

Advisory ID

CVE-2022-22509
VDE-2022-001

Vulnerability Description

The user management of the FL SWITCH 2xxx family of devices implements access rights based on roles and permission groups. An unprivileged user logged in via the SSH CLI is assigned to the admin role independent of his configured access role enabling full access to the device configuration (CWE-266 - Incorrect Privilege Assignment).

Affected products

User Management via SSH was first introduced with firmware version 3.00. Firmware versions other than 3.00 are not affected by this vulnerability.

Article no	Article	Affected version	Fixed version
2702323	FL SWITCH 2005	3.00	Download
2702324	FL SWITCH 2008	3.00	Download
2702326	FL SWITCH 2208	3.00	Download
2702327	FL SWITCH 2208	3.00	Download
2702328	FL SWITCH 2207-FX	3.00	Download
2702329	FL SWITCH 2207-FX SM	3.00	Download
2702331	FL SWITCH 2206-2FX SM	3.00	Download
2702333	FL SWITCH 2206-2FX SM ST	3.00	Download
2702330	FL SWITCH 2206-2FX	3.00	Download
2702332	FL SWITCH 2206-2FX ST	3.00	Download
2702334	FL SWITCH 2204-2TC-2SFX	3.00	Download

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel WachholzDeutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDE33XXX
IBAN:
DE93 3607 0050 0226 2665 00Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADE33XXX
IBAN:
DE31 4764 0051 0226 0396 00

2702652	FL SWITCH 2308	3.00	Download
2702653	FL SWITCH 2304-2GC-2SFP	3.00	Download
2702969	FL SWITCH 2206-2SFX	3.00	Download
2702970	FL SWITCH 2306-2SFP	3.00	Download
2702665	FL SWITCH 2105	3.00	Download
2702666	FL SWITCH 2108	3.00	Download
1009220	FL SWITCH 2308 PN	3.00	Download
1009222	FL SWITCH 2306-2SFP PN	3.00	Download
1044024	FL SWITCH 2208 PN	3.00	Download
1044028	FL SWITCH 2206-2SFX PN	3.00	Download
1044029	FL SWITCH 2216 PN	3.00	Download
1044030	FL SWITCH 2214-2SFX PN	3.00	Download
1006188	FL SWITCH 2214-2SFX	3.00	Download
1006191	FL SWITCH 2314-2SFP	3.00	Download
1031673	FL SWITCH 2316 PN	3.00	Download
1031683	FL SWITCH 2314-2SFP PN	3.00	Download
2702903	FL SWITCH 2016	3.00	Download
2702904	FL SWITCH 2216	3.00	Download
2702905	FL SWITCH 2214-2FX	3.00	Download
2702906	FL SWITCH 2214-2FX SM	3.00	Download
2702907	FL SWITCH 2212-2TC-2SFX	3.00	Download
2702908	FL SWITCH 2116	3.00	Download
2702909	FL SWITCH 2316	3.00	Download
2702910	FL SWITCH 2312-2GC-2SFP	3.00	Download
2702881	FL NAT 2008	3.00	Download
2702882	FL NAT 2208	3.00	Download
2702981	FL NAT 2304-2GC-2SFP	3.00	Download
1043412	FL SWITCH 2408	3.00	Download
1043414	FL SWITCH 2406-2SFX	3.00	Download
1043484	FL SWITCH 2508	3.00	Download
1043491	FL SWITCH 2506-2SFP	3.00	Download
1088853	FL SWITCH 2404-2TC-2SFX	3.00	Download
1088872	FL SWITCH 2504-2GC-2SFP	3.00	Download
1089133	FL SWITCH 2408 PN	3.00	Download
1089134	FL SWITCH 2508 PN	3.00	Download
1089126	FL SWITCH 2406-2SFX PN	3.00	Download
1089135	FL SWITCH 2506-2SFP PN	3.00	Download
1043416	FL SWITCH 2416	3.00	Download
1043496	FL SWITCH 2516	3.00	Download
1043423	FL SWITCH 2414-2SFX	3.00	Download
1043499	FL SWITCH 2514-2SFP	3.00	Download
1088875	FL SWITCH 2412-2TC-2SFX	3.00	Download
1088856	FL SWITCH 2512-2GC-2SFP	3.00	Download
1089150	FL SWITCH 2416 PN	3.00	Download
1089205	FL SWITCH 2516 PN	3.00	Download
1089139	FL SWITCH 2414-2SFX PN	3.00	Download

1089154	FL SWITCH 2514-2SFP PN	3.00	Download
1095627	FL SWITCH 2208C	3.00	Download
1095628	FL SWITCH 2206C-2FX	3.00	Download
1106500	FL SWITCH 2608	3.00	Download
1106616	FL SWITCH 2608 PN	3.00	Download
1106615	FL SWITCH 2708	3.00	Download
1106610	FL SWITCH 2708 PN	3.00	Download
1106707	FL SWITCH 2008F	3.00	Download
1184084	FL SWITCH 2316/K1	3.00	Download
1215329	FL SWITCH 2506-2SFP/K1	3.00	Download
1215350	FL SWITCH 2508/K1	3.00	Download

Impact

An attacker could elevate his privileges and take over control of the device.

Classification of Vulnerability

Base Score: 8.8

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Temporary Fix / Mitigation

We recommend disabling the login via SSH on devices running firmware version 3.00. If access to the CLI is required and an encrypted connection is not necessary in the specific application, the unencrypted Telnet service may be utilized, which is not affected by this vulnerability.

Remediation

Phoenix Contact strongly recommends affected users to upgrade to the current Firmware 3.10 or higher which fixes this vulnerability.

Acknowledgement

This vulnerability was discovered internally.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.