VDE-2026-126: Phoenix Contact: Privilege escalation vulnerability in the firmware of FL WLAN 23xx and FL WLAN 2x1x Devices

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed Nov 18 10:00:00 CET 2026	Engine: 2.6.16
Current release date: Wed Nov 18 10:00:00 CET 2026	Build Date: Thu Oct 29 12:01:55 CET 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 8.8	Severity: High
Original language:	Language: en-GB
Also referred to: VDE-2026-126, PCSA-2026-00021	

Summary

A vulnerability has been identified in the firmware of FL WLAN devices. A low-privileged remote attacker can change the password of arbitrary users using the REST API, including administrative accounts. By changing the administrator password, an attacker can obtain full administrative access to the device and modify all configuration settings.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

Impact

By exploiting this vulnerability, an attacker can obtain full administrative access to the device, leading to a complete loss of confidentiality, integrity, and availability.

Mitigation

FL WLAN devices are designed and developed for the use in closed industrial networks. Phoenix Contact therefore strongly recommends using the devices exclusively in closed networks and protected by a suitable firewall.

Remediation

Phoenix Contact recommends updating affected devices to firmware version 26.10, which addresses this vulnerability

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Affected Product(s)

Article	Name	Affected	Fixed
2702992	FL WLAN 1020	< 26.10	26.10
2702993	FL WLAN 1021	< 26.10	26.10
1752493	FL WLAN 1022	< 26.10	26.10
1386091	FL WLAN 1120	< 26.10	26.10
1386092	FL WLAN 1121	< 26.10	26.10
1752496	FL WLAN 1122	< 26.10	26.10
1360275	FL WLAN 2330	< 26.10	26.10
1360276	FL WLAN 2331	< 26.10	26.10
1510147	FL WLAN 2340	< 26.10	26.10
1510249	FL WLAN 2341	< 26.10	26.10

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERTVDE for coordination. (see: https://certvde.com/en/)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- pcsa-2026-00021 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- VDE-2026-126: Phoenix Contact: Privilege escalation vulnerability in the firmware of FL WLAN 23xx and FL WLAN 2x1x Devices - HTML (SELF): https://certvde.com/en/advisories/VDE-2026-126
- VDE-2026-126: Phoenix Contact: Privilege escalation vulnerability in the firmware of FL WLAN 23xx and FL WLAN 2x1x Devices - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-126.json
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed Nov 18 10:00:00 CET 2026	Initial revision.

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Vulnerability Details

Improper privilege management via REST API password change (CVE-2026-113497)

CVE description

A low-privileged remote attacker can change the password of arbitrary users using the REST API, including administrative accounts. By changing the administrator password, an attacker can obtain full administrative access to the device and modify all configuration settings.

CWE:	CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware <26.10 installed on FL WLAN 1020 Order number: 2702992	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 1120 Order number: 1386091	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 1022 Order number: 1752493	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 1122 Order number: 1752496	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 1121 Order number: 1386092	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 1021 Order number: 2702993	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 2331 Order number: 1360276	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 2341 Order number: 1510249	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 2330 Order number: 1360275	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
Firmware <26.10 installed on FL WLAN 2340 Order number: 1510147	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 26.10 installed on FL WLAN 1020 Order number: 2702992 (Download)

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Product
Firmware 26.10 installed on FL WLAN 1120 Order number: 1386091 (Download)
Firmware 26.10 installed on FL WLAN 1022 Order number: 1752493 (Download)
Firmware 26.10 installed on FL WLAN 1122 Order number: 1752496 (Download)
Firmware 26.10 installed on FL WLAN 1121 Order number: 1386092 (Download)
Firmware 26.10 installed on FL WLAN 1021 Order number: 2702993 (Download)
Firmware 26.10 installed on FL WLAN 2331 Order number: 1360276 (Download)
Firmware 26.10 installed on FL WLAN 2341 Order number: 1510249 (Download)
Firmware 26.10 installed on FL WLAN 2330 Order number: 1360275 (Download)
Firmware 26.10 installed on FL WLAN 2340 Order number: 1510147 (Download)

Acknowledgments

- Phoenix Contact for Found during internal product testing.

References

- CVSS v4.0 Score: 8.7 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany