Firmware release notes of switch series IE-SW-PL18M

Affected models:

Device name	Article No.
IE-SW-PL18M-2GC-16TX	1241320000
IE-SW-PL18MT-2GC-16TX	1286970000

Version 3.4.40 — Released: May 2025

Important Note: Please upgrade or downgrade to intermediate firmware V3.4.34 for optimizing stack size before updating to a newer version.

Bug Fixes:

- Fixed [CVE-2025-41649]: Out-of-bounds write vulnerability. This vulnerability is caused by insufficient input validation, which allows writing data beyond buffer boundaries.
- Fixed [CVE-2025-41650]: Denial-of-Service vulnerability. This vulnerability allows attackers to exploit a service, originally designed for deployment purposes.
- Fixed [CVE-2025-41651]: Missing authentication vulnerability. This vulnerability allows attackers to manipulate device configurations without requiring authentication.
- Fixed [CVE-2025-41652]: Frontend authorization logic disclosure vulnerability. Exploitation of this vulnerability could allow attackers to bypass authentication, perform brute-force or MD5 collision attacks, and gain unauthorized access to sensitive configurations or disrupt services.
- Fixed [CVE-2025-41653]: A specially crafted HTTP message header can lead to denial of service.

Version 3.4.38 — Released: February 2025

Important Note: Please upgrade or downgrade to intermediate firmware V3.4.34 for optimizing stack size before updating to a newer version.

Improvements:

- Update OpenSSL 1.0.2k to support TLS v1.2 for accessing switch´s web interface via https with current internet browsers.
- Complete serial number (12-digits) will be shown in the web interface now (applicable only from Hardware Revision V 3.0.0).

Bug Fixes:

- Fixed [CVE-2016-2183]: Weak SSL/TLS Key Exchange.
- SNMPv3 encryption key no longer visible when entering via web-interface.
- Fixed the issue of "Set device IP" function sometimes does not answer DHCP Discovery messages sent from a DHCP client, resulting in the client not being able to obtain an IP address.
- SNMPv3 access control w/o authentication was not possible.

Version 3.4.34 — Released: February 2025

- Reduce task stack size for firmware upgrade.

Version 3.4.30 — Released: November 2019

Improvements:

- Added new Search Service protocol (encrypted) to be used with new “Weidmüller Switch Configuration Utility”
- Added Management Interface page to enable/disable Search Service (unencrypted) and Search Service (encrypted) in Main Menu > Basic Settings > Security > Management Interface

Version 3.4.4 **Released: September 2016**

Improvements:

- Pass the ODVA certification of industrial protocol “EtherNet/IP”
- Pass the PI certification of industrial protocol “PROFINET RT”
- Add some minor SNMP OIDs
- Enhancement of multicast performance
- Optimized Turbo Ring redundancy performance
- Elimination of some vulnerability issues
  - Web user interface: Ping function in diagnostic menu vulnerable to XSS attack
  - Switch may reboot when using special URL to attack the web user interface
  - User account privileges could be changed by web developer plug-in of Firefox browser

Bug Fixes:

- Improvement of stability of PROFINET I/O communication
- Configuration import failed if system name was too long
- Wrong counter information of switch packets when displayed in Web interface or when read via SNMP
- Wrong message “Login Authentication failed” has been stored in the log file though login procedure was successful
- Port settings of Gigabit Combo ports are reset to default values after system reboot

Version 3.4.2 **Released: February 2016**

Improvements:

- Support of RSTP-2004
- Support of Hybrid VLAN
- RADIUS and TACACS+ for user login authentication
- RADIUS for 802.1x port authentication
- Configuration of limitation of Egress rates
- Filtering of packets with unknown unicast addresses
- CPU loading monitoring
- Change IP without reboot
- DHCP Discover retry configuration
- GARP timer adjustment
- Loop-protection
- Link Fault Shutdown (Disable mode in “Rate Limit” function)
- Implementation of SNMP-Trap (private) for loop protection
- Implementation of functionality to read diagnostic values of DDM-SFP-transceivers via private MIB-file
- Additional support of 3rd party SFP transceivers
- Implementation of industrial protocol “EtherNet/IP”
- Implementation of industrial protocol “PROFINET RT”

Bug Fixes:

- Web interface displayed errors under Java 8 environment when opening the monitoring menu (due to new Java security enhancements implemented in version 8).
- Displaying inaccurate values when reading DDM SFP transceiver diagnostic data
- Switch may reboot when using special DHCP discovery packet with multicast-type source MAC address.
- Potential of abnormal multicast transmission when enabling IGMP Snooping
- Radius based login authentication failed if the Radius server did not support privileged levels assignment
- Firmware upgrade failed when RADIUS authentication (IEEE 802.1x) was enabled
- Switch reboots when receiving IGMP v3 packets (commonly used in Windows 7)

Version 2.6.4 **Released: April 2011**

- First release