

Firmware release notes of switch series IE-SW-PL16M

Affected models:

Device name	Article No.
IE-SW-PL16M-16TX	1241100000
IE-SW-PL16MT-16TX	1286820000
IE-SW-PL16M-14TX-2SC	1241120000
IE-SW-PL16MT-14TX-2SC	1286830000
IE-SW-PL16M-14TX-2ST	1241130000
IE-SW-PL16MT-14TX-2ST	1286840000

General upgrade Information:

Upgrading from older versions to latest firmware Version 3.4.2 generally can be done without any impacts regarding the currently set switch configuration.

Version 3.4.2

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 IO 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

Version 3.2.2

Released: February 2016

New features:

- 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 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).
- Switch may reboot when using special DHCP discovery packet with multicast-type source MAC address.
- Radius based login authentication failed if the Radius server did not support privileged levels assignment
- Potential of abnormal multicast transmission when enabling IGMP Snooping

- Switch reboots when receiving IGMP v3 packets (commonly used in Windows 7)
- Firmware upgrade failed when RADIUS authentication (IEEE 802.1x) was enabled

Version 2.6.8

Released: April 2011

- First release