Firmware release notes of switch series IE-SW-VL05M

Affected models:

Device name	Article No.
IE-SW-VL05M-5TX	1504280000
IE-SW-VL05MT-5TX	1504310000

Version 3.6.36   **Released: February 2026**

Bug Fixes:

- Password unknown after config import.
- Cold start caused by HTTP access (when configured as HTTPs only).

Improvements:

- Enhance task freeze detection mechanism.
- Lengthen task freeze examination time to 120s to reduce chances of triggering watchdog.

Version 3.6.32   **Released: May 2025**

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 3.6.30   **Released: February 2025**

Bug Fixes:

- Fixed [CVE-2016-2183]: Weak SSL/TLS Key Exchange.
- SNMPv3 encryption key no longer visible when entering via web-interface.

Version 3.6.28   **Released: June 2024**

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 1.2.2).

Bug Fixes:

- 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.

Version 3.6.24   **Released: November 2019**

New features:

- Switch`s web interface can now be accessed encrypted via https
- 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
- Switch can be addressed via Modbus requests using TCP and UDP protocol

Bug Fixes:

- Fixed a bug regarding DCP handling. PROFINET device name was deleted after Switch was reset to factory settings in TIA portal

Version 3.6.6   **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
- 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
- RSTP function was incompatible with some 3rd party devices
- 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 3.3.10   **Released: November 2015**

New features:

- Implementation of industrial protocol "PROFINET RT"
- Implementation of industrial protocol "EtherNet/IP"

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).
- Traffic rate limiting setting errors when switching between "Normal mode" and "Port Disable mode"
- Improper operation of IGMP snooping when IGMP control messages are not tagged with PVID 1
- Static multicast setting errors when changing VLAN settings
- Switch reboot when port-based VLAN was enabled

Version 3.3.4   **Released: April 2014**

- First release