



Firmware for EDS-P510 Series Release Notes

Version: v3.9	Build: 21110514
Release Date: Dec 14, 2021	

Applicable Products

EDS-P510 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Upgraded OpenSSL to 1.0.2k and added support for TLS v1.2.
- Added a memory usage protection function for certain configurations.
- Added an additional encryption option and command to the web UI and CLI.
- Added the “Set” function for standard MIB ifAdminStatus.
- Increased the number of RSTP nodes to 40.

Bugs Fixed

- When Turbo Ring V2 is working alongside Turbo Chain, and the Head Port link turns on or off, the recovery time increases to < 50 ms.
- Turbo Ring V1 does not work with RSTP Force Edge port.
- The system reboots when reading or writing SNMP OID 1.3.6.1.2.1.2.2.1.1.4294967295.
- Turbo Ring V1 does not work properly.
- Accessing LLDP via Telnet causes the device to reboot.
- SNMP responds slowly when querying the MAC table.
- Disabling the Broadcast Storm Control Port function does not work.
- The ABC-01 does not function properly.
- Some counters show incorrect negative values.
- Some counters show abnormal values after resetting.
- The LLDP configuration webpage is vulnerable to javascript injections.
- Reading speeds are slow when adding a new MAC address.
- IEEE 802.1x authentication may fail under certain conditions.
- The "copy startup-config" CLI command causes the system to restart.
- If Turbo Chain is enabled and the Rate Limit function is configured on the Head Port, the Turbo Chain would become unstable.
- The SFP fiber link behaves abnormally under certain conditions.
- The “get bulk” SNMP command does not work properly for some OIDs.
- TACACS+ authentication would fail under certain conditions.
- OID 1.3.6.1.2.1.17.4.3.1.1 causes the “get” SNMP command to time out.
- The RSTP configuration is missing.
- The Ping function and SNMP do not respond.
- The system does not synchronize the system time with the real-time clock (RTC).
- Establishing an SSH connection may cause the system to reboot.
- [MSRV-2017-001][CVE-2019-6518] Plain text storage of a password.
- [MSRV-2017-003][CVE-2019-6526] Missing encryption of sensitive data.
- [MSRV-2017-004][CVE-2019-6524] Improper restriction of excessive authentication attempts.
- [MSRV-2017-005][CVE-2019-6559] Resource exhaustion.
- [MSRV-2017-006][CVE-2019-6557] Buffer overflow in endpoint.



- [MSRV-2017-007][CVE-2019-6522] Device Memory Read.
- [MSRV-2017-009][CVE-2019-6565] Multiple XSS.
- [MSRV-2017-011][CVE-2019-6561] Cross-Site Request Forgery (CSRF).
- [MSRV-2017-013] Use of a broken or risky cryptographic algorithm.
- [MSRV-2017-014] Use of hard-coded cryptographic key.
- [MSRV-2017-015] Use of hard-coded password.
- [MSRV-2017-018] Weak password requirements.
- [MSRV-2017-019] Information exposure.
- [MSRV-2017-020][CVE-2017-13703] Buffer overflow in the session ID.
- [MSRV-2017-021][CVE-2017-13702] Cookie management.
- [MSRV-2017-022][CVE-2017-13700] Cross-site scripting (XSS).
- [MSRV-2017-026] Use of a broken or unsecure cryptographic algorithm.
- [MSRV-2019-002] XSS vulnerability in the LLDP diagnostic page.
- [MSRV-2019-003] Denial of Service (web service) by improper HTTP GET command.
- [MSRV-2019-004] Denial of Service (web service) by over-sized firmware upgrade through HTTP/HTTPS.
- [MSRV-2019-005] Denial of Service (web service) by excessive length of HTTP GET command.

Changes

N/A

Notes

- MSRV is Moxa's internal security vulnerability tracking ID.



Version: v3.8	Build: Build_17041115
Release Date: May 04, 2017	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Add warning message when default password was not changed
- Encrypt security Keys in user interface
- Enhance RSTP compatibility

Bugs Fixed

- Cross-site scripting vulnerability.
- Denial of Service attack vulnerability.
- Privilege escalation vulnerability.
- SSL v2/v3 vulnerability in https.
- Web console cannot be accessed due to SNMP get bulk.
- Specific CLI command cause switch reboot with default settings.
- Add a new VLAN will change IGMP querier state from disable to enable.
- Saving configuration to ABC-01 cannot be performed via IE browser.
- Rate limit cannot be set in web UI.
- Telnet hangs after SSH disabled.
- Correct RSTP edge definition in exported configuration file.
- Correct authorization of Radius/TACACS+ login.
- Correct RSTP Auto-Edge behavior.
- After upgrade firmware, the system maybe warm start when the user login the switch

Changes

N/A

Notes

N/A