



## Firmware for EDS-P510A Series Release Notes

<b>Version:</b> v3.11	<b>Build:</b> 24011616
<b>Release Date:</b> Feb 07, 2024	

### **Applicable Products**

EDS-P510A Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Enhanced the firmware memory allocation mechanism.
- Improved the handshake mechanism for establishing port links.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.10</b>	<b>Build: 23062906</b>
<b>Release Date: Aug 31, 2023</b>	

### **Applicable Products**

EDS-P510A Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added support for additional management interfaces: HTTP, HTTPS.
- Added compatibility with certain non-standard BPDU to prevent broadcast storm.
- If the "TURBO RING" DIP switch is set to ON, only two ports will now be reserved for Turbo Ring. If both the "TURBO RING" and "COUPLER" DIP switches are set to ON, four ports will be reserved.
- When disabling Modbus TCP or Ethernet/IP, the relevant TCP ports (#502 and #44818) will now also be disabled.
- Removed the HTTPS warning for Chrome and Edge browsers when importing the RootCA.

### **Bugs Fixed**

- The "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.
- Users are sometimes unable to connect to the system via SSH.
- The system will unintentionally perform a cold start when using N-Snap to log in via SSH.
- [CVE-2022-40691] A specially crafted HTTP request can lead to disclosure of sensitive information.
- [CVE-2022-40214] Potential tampered messages.
- [CVE-2022-40224] A specially-crafted HTTP message header can lead to denial of service.

### **Changes**

- Removed the "recommended browser" message from the web interface.
- The TACACS+ and RADIUS shared keys and SNMPv3 data encryption key are now cleared after modifying specific configurations (e.g. TACACS+/RADIUS login list, SNMP version, SNMP authentication/encryption method).
- Changed the displayed name of the RADIUS authentication mechanism from EAP-MD5 to PAP.

### **Notes**

N/A



<b>Version: v3.9</b>	<b>Build: 21110514</b>
<b>Release Date: Dec 14, 2021</b>	

## Applicable Products

EDS-P510A 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 SNMP Trap for PoE events contains an incorrect parameter.
- If Flow Control is enabled on Gigabit ports, traffic on these ports is blocked.
- The SFP port description is incorrect.
- 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.
- Due to memory reallocation for the items listed under “Enhancements”, please follow one of the methods below when upgrading to firmware v3.9:
  - a. Clear all syslog and upgrade to the new firmware through the web UI.
  - b. Consult Moxa Technical Support for assistance.



<b>Version: v3.8</b>	<b>Build: Build_17041115</b>
<b>Release Date: May 04, 2017</b>	

### **Applicable Products**

EDS-P510A-8PoE-2GTXSFP, EDS-P510A-8PoE-2GTXSFP/KC, EDS-P510A-8PoE-2GTXSFP-T, EDS-P510A-8PoE-2GTXSFP-T/KC

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added warning message when default password was not changed.
- Encrypted security keys in the user interface.
- Enhanced 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 when the SNMP get bulk service is running.
- Specific CLI command caused the switch to 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.
- Corrected RSTP edge definition in exported configuration file.
- Corrected authorization of Radius/TACACS+ login.
- Corrected RSTP Auto-Edge behavior.
- After the firmware has been upgraded, the system may perform a warm start when the user logs in to the switch.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.5</b>	<b>Build: Build_15051416</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

EDS-P510A-8PoE-2GTXSFP, EDS-P510A-8PoE-2GTXSFP/KC, EDS-P510A-8PoE-2GTXSFP-T, EDS-P510A-8PoE-2GTXSFP-T/KC

### **Supported Operating Systems**

N/A

### **New Features**

- Added new Multicast Fast Forwarding Mode.

### **Enhancements**

- Increased IGMP Groups to 1024 (original 256 groups).
- Improved Turbo Chain link status check mechanism at the head port.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.4</b>	<b>Build: Build_15010916</b>
<b>Release Date: N/A</b>	

**Applicable Products**

EDS-P510A-8PoE-2GTXSFP, EDS-P510A-8PoE-2GTXSFP/KC, EDS-P510A-8PoE-2GTXSFP-T, EDS-P510A-8PoE-2GTXSFP-T/KC

**Supported Operating Systems**

N/A

**New Features**

N/A

**Enhancements**

N/A

**Bugs Fixed**

- Web user interface displayed errors under Java 8 environments.

**Changes**

N/A

**Notes**

N/A



<b>Version: v3.3</b>	<b>Build: N/A</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

EDS-P510A-8PoE-2GTXSFP, EDS-P510A-8PoE-2GTXSFP/KC, EDS-P510A-8PoE-2GTXSFP-T, EDS-P510A-8PoE-2GTXSFP-T/KC

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Added web interface for loop-protection enable/disable.
- Added web interface for SSH/SSL key generation.
- Added SNMP MIB for SFP DDM (Diagnostics).
- Added web interface/CLI/SNMP for NTP/SNTP client settings.

### **Bugs Fixed**

- Login failed in CLI mode when the password contained special characters.
- Hybrid VLAN lacked an SNMP MIB object.
- SFP DDM (Diagnostics) displayed inaccurate values.
- IEEE 1588 PTP did not function correctly.
- The configuration import was restricted if the system name was too long.
- Login authentication failed if the radius server did not support privilege levels assignment.
- DIP switch "Coupler" On/Off is malfunction.

### **Changes**

N/A

### **Notes**

N/A





<b>Version: v3.1</b>	<b>Build: N/A</b>
<b>Release Date: N/A</b>	

**Applicable Products**

EDS-P510A-8PoE-2GTXSFP, EDS-P510A-8PoE-2GTXSFP/KC, EDS-P510A-8PoE-2GTXSFP-T, EDS-P510A-8PoE-2GTXSFP-T/KC

**Supported Operating Systems**

N/A

**New Features**

- New release for the EDS-P510A-8PoE Series.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A