



## Firmware for EDS-405A Series (PTP models) Release Notes

<b>Version: v3.10</b>	<b>Build: 23061800</b>
<b>Release Date: Aug 31, 2023</b>	

### Applicable Products

EDS-405A-PTP, EDS-405A-PTP-T

### Supported Operating Systems

N/A

### New Features

N/A

### Enhancements

- Added support for TLS v1.3.
- 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.
- When using 1588 PTP with E2E BC model, the system will unexpectedly perform a warm start.

### 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: 22011419</b>
<b>Release Date: Mar 24, 2022</b>	

## Applicable Products

EDS-405A-PTP 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.
- Added support for HTTPS, SSH, and SSL.

## 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.
- 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 Turbo Chain recovery time is irregular during warm and cold starts.
- 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-2017-013] 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.



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

### **Applicable Products**

EDS-405A-PTP

### **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.

### **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 caused switch to reboot with default settings.
- Adding a new VLAN changed IGMP querier state from disabled to enabled.
- Saving configurations to ABC-01 could not be performed via IE browser.
- Rate limit could not 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.
- System could only reboot after a period of operation while PROFINET was enabled.
- After the firmware has been upgraded, the system sometimes performed a warm start when the user logged in to the switch.

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v3.5</b>	<b>Build: Build_15040918</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

EDS-405A-PTP

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

N/A

### **Bugs Fixed**

- Ethernet ports auto-negotiation fail at 10 M speed.
- 1588 PTP time synchronization failed after rebooting grandmaster clock.
- Unable to configure system name via SNMP.

### **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-405A-PTP

**Supported Operating Systems**

N/A

**New Features**

- First release for EDS-405A-PTP Series.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A