Firmware for EDS-405A Series Release Notes

Version: v3.14	**Build: 24011614**
Release Date: Feb 03, 2024	

Applicable Products

EDS-405A 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

Version: v3.13	Build: N/A
Release Date: Sep 27, 2023	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- The switch cannot be accessed via HTTP.

Changes

N/A

Notes

N/A

Version: v3.12	Build: 23061723
Release Date: Aug 31, 2023	

Applicable Products

EDS-405A Series

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 unintentially 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).

Notes

N/A

Version: v3.11	Build: 21110512
Release Date: Dec 14, 2021	

Applicable Products

EDS-405A 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.
- The "copy startup-config" CLI command causes the system to restart.
- The “get bulk” SNMP command does not work properly for some OIDs.
- 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.

Version: v3.10	**Build: EDS405A_V3.10_Build_19121910**
Release Date: Jan 06, 2020	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

- Added support for HTTPS, SSH, and SSL.
- Added support for new Moxa commands.
- Added support for RSTP up to 40 nodes.
- Added the Management Interface configuration page.

Enhancements

- The default password has changed to "moxa" instead of the field being empty. In addition, for security reasons, the minimum password length must not be less than 4 characters.
- Modified the Java applet to XML and HTML.
- Added memory protection.
- Added support for SNMP Set for standard MIB ifAdminStatus.
- Improved Turbo Ring V2 and Turbo Chain recovery times.
- [MSRV-2017-001][CVE-2019-6518] Added encrypted Moxa service with enable/disable button on GUI to support communication over encrypted commands with MXconfig/MXview.
- [MSRV-2017-002][CVE-2019-6563] Supports random salt to prevent session prediction attack of HTTP/HTTPS.
- [MSRV-2017-003, 004, 005][CVE-2019-6526, 6524, 6559] Added encrypted Moxa service with enable/disable button on GUI to support communication over encrypted commands with MXconfig/MXview.
- [MSRV-2017-011][CVE-2019-6561] Supports browser cookie parameters “same-site” to eliminate CSRF attacks.
- [MSRV-2017-013] [CWE-327] Supports system configuration file encryption mechanism.
- [MSRV-2017-017] Supports HTTPS for secure communication to avoid confidential information being transmitted through clear text.
- [MSRV-2017-021][CVE-2017-13702] Release the cookie once the session expires to avoid the old cookie value being reused.
- [MSRV-2017-022][CVE-2017-13700] Avoid XSS (Cross-site Scripting) attack by regulating the input parameters’ format.
- [MSRV-2017-023] Supports configuration backup encryption mechanism to prohibit confidential information from being disclosed.
- [MSRV-2019-002] Avoids XSS (Cross-site Scripting) attack by regulating the input parameters’ format of the LLDP diagnostic page.

Bugs Fixed

- Turbo Ring V1 does not work with RSTP force edge ports.
- SNMP would reboot the system when adding OID 1.3.6.1.2.1.2.2.1.1.4294967295.
- Turbo Ring V1 not working properly.
- The system would reboot when connecting through Telnet when LLDP is enabled and transmitting.
- Storm control would sometimes fail to disable a problematic port.
- ABC-01 not working properly.
- Unusual counter behaviour issue.
- Issue with Javacript injection.
- Slow SNMP response when reading MAC Address table (OID 1.3.6.1.2.1.17.4.3.1.1)

- The system would reboot when entering specific CLI commands.
- Slow SNMP response when pinging a client.
- Slow Turbo Chain warm/cold start recovery time.
- [MSRV-2017-001][CVE-2019-6518] Plain text storage of a password.
- [MSRV-2017-002][CVE-2019-6563] Predictable Session ID.
- [MSRV-2017-003][CVE-2019-6526] Sensitive data was not encrypted.
- [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 vulnerabilities that may allow remote control.
- [MSRV-2017-009][CVE-2019-6565] No proper validation of user inputs, which allows users to perform XSS attacks.
- [MSRV-2017-011][CVE-2019-6561] CSRF attacks were possible if browser cookie parameters were not correct.
- [MSRV-2017-012] [CWE-121] An attacker could exploit the improper boundary check vulnerability to perform DoS or execute arbitrary codes.
- [MSRV-2017-013] [CWE-327] Administrative credentials could be disclosed.
- [MSRV-2017-014] [CWE-321] A hard-coded crypographic key was used.
- [MSRV-2017-015] [CWE-798] Engineering troubleshooting shortcut with predefined common string.
- [MSRV-2017-016] [CWE-120] Abnormal device operations.
- [MSRV-2017-017] Confidential information can be transmitted using clear text.
- [MSRV-2017-018] [CWE-521] Weak password policy.
- [MSRV-2017-019] [CWE-200] Information was available before a user logged in.
- [MSRV-2017-020][CVE-2017-13703] The input parameter length of web cookies (session, account, password) was not checked.
- [MSRV-2017-021][CVE-2017-13702] Old cookie was reused.
- [MSRV-2017-022][CVE-2017-13700] XSS (Cross-site Scripting) attack.
- [MSRV-2017-023] Confidential information could be disclosed.
- [MSRV-2017-024] [CVE-2017-13698] Public and private key can be extracted from the firmware binary.
- [MSRV-2017-025] [CVE-2017-13699] Support HTTPS to protection the password encryption algorithm
- [MSRV-2017-026] [CWE-327] A broken or risky cryptographic algorithm was used.
- [MSRV-2019-001] Devices in default mode shared one hard-coded root CA certificate.
- [MSRV-2019-002] XSS (Cross-site Scripting) attack.

Changes

N/A

Notes

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

Version: v3.8	**Build: Build_17051216**
Release Date: Jun 29, 2017	

Applicable Products

EDS-405A-T, EDS-405A, EDS-405A-EIP, EDS-405A-MM-SC, EDS-405A-MM-ST, EDS-405A-SS-SC-T, EDS-405A-MM-SC-T, EDS-405A-SS-SC, EDS-405A-EIP-T, EDS-405A-MM-ST-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- User account login authentication error in menu console mode.
- Unstable connection when using fiber links.

Changes

N/A

Notes

N/A

Version: v3.7	Build: Build_17031513
Release Date: Mar 15, 2017	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Added warning message when default password was not changed.
- Encrypted 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 the switch to reboot with default settings.
- Added 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.
- Corrected RSTP edge definition in exported configuration file.
- Corrected RSTP Auto-Edge behavior.
- Web console is inaccessible after changing VLAN setting.
- Configure LLDP via MXconifg cause SNMP module hangs.
- Cannot set password via MXconfig.

Changes

N/A

Notes

N/A

Version: v3.6	Build: Build_15080712
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- Turbo Ring/Turbo Chain operate unstably after the switch performs a warm start.
- RSTP function was incompatible with some third party devices.
- Switch configuration export error via CLI.
- Switch packet counter information error via SNMP polling.
- Web user interface Diagnosis > Ping page is vulnerable to XSS attack.
- Switch may reboot when using special URL to attack web user interface.
- User account privileges can be changed by Firefox browser web developer plugin.

Changes

N/A

Notes

N/A

Version: v3.5	Build: Build_14121009
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- Web user interface display errors under Java 8 environments

Changes

N/A

Notes

N/A

Version: v3.4	Build: N/A
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- Switch rebooted when port-based VLAN is enabled.
- Network looping when IPv6 based computer connects to Turbo Ring or Turbo Chain network.
- Traffic rate limiting setting errors when switching between Normal mode and Port Disable mode.
- IGMP snooping operated incorrectly when IGMP control messages were not with PVID 1.
- Static multicast setting errors when changing VLAN settings.
- Configuration import/export errors in CLI mode.

Changes

N/A

Notes

N/A

Version: v3.3	Build: Build_13070416
Release Date: Jul 09, 2013	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Added a web interface for loop protection enable/disable.
- Added a web interface for SSH/SSL key generation.

Bugs Fixed

- Log in failed in the CLI mode when the password contained a special character.
- Hybrid VLAN lacked the SNMP MIB object.
- IEEE 1588 PTP did not function correctly.

Changes

N/A

Notes

N/A

Version: **v3.1**	**Build:** **N/A**
Release Date: **Sep 28, 2012**	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- Passed ODVA EtherNet/IP certificate.
- Added some minor SNMP OIDs.
- Enhanced multicast performance.
- Added version number in MIB file.

Bugs Fixed

- NTP cannot synchronize time in default setting.
- NTP client function cannot work with Windows XP NTP server.
- Switch reboots when receiving IGMP v3 packets (commonly used in Windows 7).

Changes

N/A

Notes

N/A

Version: v3.0	Build: N/A
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

- RSTP-2004.
- NTP Server/Client.
- Hybrid VLAN.
- Command Line Interface.
- EtherNet/IP.
- Egress rate limit.
- Unknown unicast filtering.
- 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).

Enhancements

N/A

Bugs Fixed

- IGMP snooping chip issue problem.

Changes

- Changed default password to "moxa".

Notes

N/A

Version: v2.7	Build: N/A
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

- Added IGMP Snooping function.
- Added IEEE 802.1Q VLAN function.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v2.6	**Build: N/A**
Release Date: Dec 24, 2009	

Applicable Products

EDS-405A, EDS-405A-MM-ST, EDS-405A-MM-SC, EDS-405A-SS-SC, EDS-405A-T, EDS-405A-SS-SC-T, EDS-405A-EIP, EDS-405A-EIP-T, EDS-405A-MM-SC-T, EDS-405A-MM-ST-T

Supported Operating Systems

N/A

New Features

- 1. Supports TurboPack™ 2009 (Add the new managed functions of Turbo Chain, IPv6, Modbus/TCP, IEEE 1588 PTP, SNMP Inform, LLDP, DHCP Option 82, Firefox, and SSH)
- Add new Turbo Ring (Turbo Ring V2) Function
- Add new Ring Coupling Function
- Add Daylight Saving Function

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

For products with firmware prior to v2.6, users must upgrade to v2.6 before upgrading to the latest v3.X firmware.

Version: v1.3	**Build: N/A**
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

- Added Syslog function.
- Added Restart function.
- ABC-01 supported.
- Change default settings of Flow Control from Enabled to Disabled.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v1.1	**Build: N/A**
Release Date: N/A	

Applicable Products

EDS-405A Series

Supported Operating Systems

N/A

New Features

- First release for EDS-405A Series.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A