Firmware for EDS-408A Series Release Notes

Version: v3.14	Build: 24011518
Release Date: Feb 03, 2024	

Applicable Products

EDS-408A 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: 23061800
Release Date: Aug 31, 2023	

Applicable Products

EDS-408A 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 SNMPv3 data encryption key is now cleared after modifying specific configurations (e.g. SNMP version, SNMP authentication/encryption method).

Notes

N/A

Version: v3.12	Build: N/A
Release Date: Jan 03, 2023	

Applicable Products

EDS-408A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

N/A

Changes

Added support for second source chip.

Notes

N/A

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

Applicable Products

EDS-408A 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.
• Importing the Turbo Ring Coupling configuration fails under certain conditions.
• 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: EDS408A_V3.10_Build_19121910
Release Date: Jan 06, 2020	

Applicable Products

EDS-408A 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.

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.
• Slow SNMP response time.
• Storm control would sometimes fail to disable a problematic port.
• ABC-01 not working properly.
• The system freezes when the event log is cluttered.
• Unusual counter behaviour issue.
• Issue with Javacript injection.

- Slow SNMP response when adding a new MAC address.
- 802.1x Request Identify.would sometimes fail to retrieve authentication information.
- The system would reboot when entering specific CLI commands.
- Unstable Turbo Chain behavior when rate limiting is enabled.
- Unstable connection when using fiber links.
- System would reboot when using the SNMP Get Bulk command.
- TACACS authentication would fail under certain conditions.
- SNMP Get would timeout when using OID 1.3.6.1.2.1.17.4.3.1.1.
- The system not saving user RSTP settings.
- Slow SNMP response when pinging a client.
- Error when importing Turbo Ring coupling configuration.
- [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-2017-007][CVE-2019-6522] An attacker could read device memory on arbitrary addresses.
- [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-2017-026] [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-408A-PN, EDS-408A-PN-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• User account login authentication error in menu console mode.

Changes

N/A

Notes

N/A

Version: v3.7	Build: Build_17031513
Release Date: N/A	

Applicable Products

EDS-408A-PN, EDS-408A-PN-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Added warning message when the default password was not changed.
• Encrypted security keys in the user interface.

Bugs Fixed

• Cross-site scripting vulnerability.
• Denial of Service attack vulnerability.
• Privilege escalation vulnerability.
• SSL v2/v3 vulnerability in HTTPS.
• Web console could not be accessed due to SNMP get bulk.
• Specific CLI command caused the switch to reboot with default settings.
• Adding a new VLAN changed the IGMP querier state from disable to enable.
• Saving configurations to the ABC-01 could not 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.
• System sometimes rebooted after a period of operation when PROFINET was enabled.

Changes

N/A

Notes

N/A

Version: v3.2	Build: Build_14121010
Release Date: N/A	

Applicable Products

EDS-408A-PN, EDS-408A-PN-T

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

Version: v3.1	Build: N/A
Release Date: N/A	

Applicable Products

EDS-408A-PN, EDS-408A-PN-T

Supported Operating Systems

N/A

New Features

• First release for the EDS-408A-PN Series.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A