Firmware for EDS-516A Series Release Notes

Version: v3.14	Build: 26030320
Release Date: Mar 31, 2026	

Applicable Products

EDS-516A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• [MPSA-259470] Enhance SSH weak algorithm. Use ecdsa-sha2-nistp256 instead of ssh_rsa.key.

Bugs Fixed

• The web interface is not accessible via HTTPS when using an IPv6 address.
• Changing the password does not automatically redirect users to the login screen.
• The web interface becomes inaccessible after changing the password policy.
• [CVE-2020-11868] ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.
• Logging into the RADIUS server fails if the username is longer than 8 bytes.

Changes

N/A

Notes

N/A

Version: v3.13	Build: N/A
Release Date: Dec 03, 2025	

Applicable Products

EDS-516A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• When enabling Turbo Chain, the link on designated Turbo Chain ports goes down.

Changes

N/A

Notes

• Due to practical limitations, manually upgrading to firmware v3.13 is only available for models with hardware version v3.0 or later.

Version: v3.12	Build: N/A
Release Date: Sep 23, 2025	

Applicable Products

EDS-516A Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Added support for the SSL certificate import CLI command.
• Users can now get the device serial number via SNMP.
• Added support for login failure lockout when accessing the web interface via SSH.

Bugs Fixed

• [MPSA-245831] Enhanced the SSH cryptographic algorithm for improved security.
• Connecting the device to an HSR network over RSTP causes looping.
• The Modbus port information shows an incorrect port status when the port is not in use.
• When repeatedly restarting a Turbo Chain Member switch, the Turbo Chain may occasionally experience looping or the Member switch may become inaccessible.
• The SNMP object ifLastChange shows an incorrect value after the interface status changes.
• The bandwidth utilization shows incorrect information for some ports.
• [CVE-2023-2650] Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow.
• [CVE-2015-9251] jQuery versions prior to v3.0.0 may be vulnerable to Cross-site Scripting attacks.
• [CVE-2019-11358] jQuery versions prior to v3.4.0 mishandle jQuery.extend because of Object.prototype pollution.
• [CVE-2020-11022] [CVE-2020-11023] jQuery versions later than v1.2 and prior to v3.5.0 may execute untrusted code when passing HTML from untrusted sources."
• Partial MAC addresses cannot be read by the SNMP MIB Browser.
• The PVID cannot be configured in VLAN Hybrid mode.
• [Nessus-85582] The web application is potentially vulnerable to Clickjacking.
• Upgraded the encryption algorithm for SSL certificate key generation.
• Enhanced the SSH cipher suite.
• Users are unable to log in via HTTPS after performing a firmware upgrade.
• [CVE-1999-0524] Answering ICMP timestamp requests might lead to remote date disclosure.
• Upgraded the encryption hash for the web login cookie from MD5 to SHA-2.
• The device may perform a cold start when the SSH algorithm mismatches.
• [CVE-2024-12297] Frontend authorization logic disclosure vulnerability.
• When repeatedly restarting a Turbo Ring Slave switch, the Turbo Ring may occasionally experience looping.
• The Management Interface and System Information pages are vulnerable to XSS.
• [CVE-2002-20001] Enhanced the SSH cryptographic algorithm for improved security.
• RADIUS login authentication will fail if the username includes special characters.
• When deleting the VLAN ID associated with a trunk port in the web interface, the VLAN ID for the trunk port incorrectly shows as VLAN 0 in the CLI.
• [CVE-2025-1680] Prevent host header injection in the web interface.
• [CVE-2024-7695] An out-of-bounds write vulnerability caused by insufficient input validation allows attackers to overwrite memory beyond the buffer's bounds.
• [CVE-2024-9404] Due to insufficient input validation, exploitation of the moxa_cmd service could

lead to denial-of-service or service crashes.
• [CVE-2024-9137] Attackers could execute specified commands to perform unauthorized downloads or uploads of configuration files and system compromise.

Changes

• Changed the recommended request packet interval (RPI) setting to 1000 ms.
• SNMP is now disabled by default.
• Modbus is now disabled by default.
• Removed the PTP function.

Notes

N/A

Version: v3.11	Build: 24011623
Release Date: Feb 03, 2024	

Applicable Products

EDS-516A 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

• Due to hardware limitations, manually upgrading to firmware v3.11 or later is only available for models with hardware version v3.0 or later.

Version: v3.10	Build: 23061803
Release Date: Aug 31, 2023	

Applicable Products

EDS-516A 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 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

Version: v3.9	Build: 21110513
Release Date: Dec 14, 2021	

Applicable Products

EDS-516A 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.
• 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 “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.
• 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 03, 2017	

Applicable Products

EDS-516A-T, EDS-516A-MM-ST-T, EDS-516A-MM-ST, EDS-516A-MM-SC, EDS-516A, EDS-516A-MM-SC-T

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

Version: v3.6	Build: Build_15091011
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Turbo Ring/Turbo Chain operated unstably after switch performed a warm start.
• Switch packet counter information error via SNMP polling or web user interface display.
• Switch failed to respond to SNMP request.
• Web user interface diagnosis > Ping page is vulnerable to XSS attack.
• Switch sometimes rebooted when using special URL to attack web user interface.
• User account privileges could be changed via Firefox browser web developer plugin.
• The switch sometimes rebooted when using special DHCP discovery packet with multicast-type source MAC address.
• The switch failed to respond to DHCP discovery packets with special client-ID option values.
• Optimized Turbo Ring network performance on platform with hardware revisions before v3.0.

Changes

N/A

Notes

N/A

Version: v3.5	Build: Build_14121010
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Web user interface displayed errors under Java 8 environment.

Changes

N/A

Notes

N/A

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

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Potential multicast transmission was abnormal when enabling IGMP Snooping.
• 802.1x setting and rate-limiting functions did not work properly after exporting configuration files.

Changes

N/A

Notes

N/A

Version: v3.3	Build: N/A
Release Date: N/A	

Applicable Products

EDS-516A

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 web interface/CLI/SNMP for NTP/SNTP client settings3

Bugs Fixed

- Login failed in CLI mode when password contained special characters
- Hybrid VLAN lacks SNMP MIB object
- IEEE 1588 PTP did not function correctly
- 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 malfunction

Changes

- Supports new Moxa CPU platform

Notes

N/A

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

Applicable Products

EDS-516A

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 did not synchronize time in default settings.
- NTP client function did not work with Windows XP NTP server.
- Failed to upgrade firmware when IEEE 802.1x was enabled.
- Switch rebooted 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-516A

Supported Operating Systems

N/A

New Features

- RSTP-2004.
- MSTP.
- NTP Server/Client.
- IEEE 1588 PTP V2.
- RADIUS and TACACS+ for user login authentication.
- RADIUS for 802.1x port authentication.
- 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

N/A

Changes

N/A

Notes

N/A

Version: v2.6	Build: N/A
Release Date: Feb 23, 2010	

Applicable Products

EDS-516A, EDS-516A-MM-ST, EDS-516A-MM-SC, EDS-516A-MM-SC-T, EDS-516A-MM-ST-T, EDS-516A-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Enhance Turbo Chain function

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: v2.5	Build: N/A
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

• Supports TurboPack™ 2009 (add new functions for Turbo Chain, IPv6, Modbus/TCP, IEEE 1588 PTP, SNMP Inform, LLDP, DHCP Option 82, Firefox, and SSH).

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v2.3	Build: N/A
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Fixed bug of the learned multicast address from IGMP Snooping will be aged out after few minutes.

Changes

N/A

Notes

N/A

Version: v2.1	Build: N/A
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

• Added new Turbo Ring (“Turbo Ring V2”) function.
• Added new Ring Coupling function.
• Added Daylight Saving function.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v1.0	Build: N/A
Release Date: N/A	

Applicable Products

EDS-516A

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A