Firmware for EDS-616 Series Release Notes

Version: v3.14	Build: N/A
Release Date: Mar 31, 2026	

Applicable Products

N/A

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.
• When enabling Turbo Chain, the link on designated Turbo Chain ports unintentionally goes down.
• 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: Sep 23, 2025	

Applicable Products

EDS-616 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• Migrated to 64-bit integers to circumvent the year 2038 limitation.
• 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-2025-1680] Prevent host header injection in the web interface.
• [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.
• Standard MIB related OID returns incorrect data.
• [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.

Notes

N/A

Version: v3.12	Build: 24011615
Release Date: Feb 07, 2024	

Applicable Products

EDS-616 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: v3.11	Build: 23061805
Release Date: Aug 31, 2023	

Applicable Products

EDS-616 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 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).
• Changed the displayed name of the RADIUS authentication mechanism from EAP-MD5 to PAP.

Notes

N/A

Version: v3.10	Build: 22031515
Release Date: Mar 24, 2022	

Applicable Products

EDS-616 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.
• 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.

Version: v3.8	Build: 17041115
Release Date: May 04, 2017	

Applicable Products

EDS-616 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.
- 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 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.
- Can not save configurations to the ABC-01 via IE browser.
- Rate limit could not be set in web UI.
- PTP timestamp error in announce Message.
- Telnet hangs after SSH disabled.
- Corrected RSTP edge definition in exported configuration file.
- Corrected authorization of Radius/TACACS+ login.
- Display issue with JAVA applet.
- Corrected RSTP Auto-Edge behavior.
- System rebooted after specific CLI command.

Changes

N/A

Notes

N/A

Version: v3.4	Build: 15011510
Release Date: N/A	

Applicable Products

EDS-616 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: v3.3	Build: 13092410
Release Date: N/A	

Applicable Products

EDS-616 Series

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 the CLI mode when the password contained a special character.
- Hybrid VLAN lacked SNMP MIB object.
- SFP DDM (Diagnostics) displayed inaccurate values.
- IEEE 1588 PTP did not function correctly.
- Far-end fault failed on 100 M fiber port.
- Importing configurations 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 malfunctioned.

Changes

N/A

Notes

N/A

Version: v3.1	Build: 12092817
Release Date: N/A	

Applicable Products

EDS-616 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 could not synchronize time in default settings.
- NTP client function could not work with Windows XP NTP server.
- Firmware Upgrade Failed when IEEE 802.1x was enabled.
- The 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-616 Series

Supported Operating Systems

N/A

New Features

- RSTP-2004.
- MSTP.
- NTP Server/Client 4.SW 1588 PTPv2.
- CLI.
- Ethernet/IP.
- Hybrid VLAN.
- Radius/Tacacs+ for both login access and port authentication
- Egress rate limit.
- CPU loading.
- Change IP address without rebooting.
- DHCP Discover retries forever, or retries for a period of time.
- GARP timer adjustment.
- Loop-protection.
- Rate Limit: port disable mode.

Enhancements

N/A

Bugs Fixed

- Event log display “module 3 & 4 inserted” issue.

Changes

N/A

Notes

N/A

Version: v1.2	Build: N/A
Release Date: N/A	

Applicable Products

EDS-616 Series

Supported Operating Systems

N/A

New Features

• Added hot swap function.
• Supports the CM-600-4TX-PTP module for IEEE 1588 v1/v2 protocol. Please download the latest firmware (1.3 or above) for the CM-600- 4TX-PTP module to avoid any unexpected abnormal functions.

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-616 Series

Supported Operating Systems

N/A

New Features

• Added hot swappable function for supporting hot-plug interface modules.

Enhancements

N/A

Bugs Fixed

• After the time setting of Age Time was changed, the function did not work normally.

Changes

N/A

Notes

N/A

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

Applicable Products

EDS-616 Series

Supported Operating Systems

N/A

New Features

• New firmware release for EDS-616 Series.
• 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