



Firmware for EDS-518E Series Release Notes

Version: v6.2	Build: N/A
Release Date: Sep 15, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

- Supports Interface Tracking, Ping Tracking, and Logic Tracking.
- Supports many-to-many port mirroring.

Enhancements

- The CPU utilization now displays a percentage instead of "Normal" and "Busy".
- Firmware upgrade processing status is displayed.
- Email addresses can contain up to 39 characters.
- Email Mail Servers can contain up to 39 characters.
- Enhanced SSH with secure key exchange algorithm, Diffie-Hellman Group 14.
- Improved random distribution of TCP Initial Sequence Number (ISN) values.

Bugs Fixed

- [MSRV-2017-002][CVE-2019-6563] Predictable Session ID: Supports random salt to prevent session prediction attack of HTTP/HTTPS.
- [MSRV-2017-003][CVE-2019-6526] Encryption of sensitive data is missing: Supports encrypted Moxa service with enable/disable button on the GUI to support the communication of encrypted commands with MXconfig/MXview.
- [MSRV-2017-004][CVE-2019-6524] Improper restriction of excessive authentication attempts: Supports encrypted Moxa service with enable/disable button on the GUI to support the communication of encrypted commands with MXconfig/MXview.
- [MSRV-2017-005][CVE-2019-6559] Resource exhaustion: Supports encrypted Moxa service with enable/disable button on the GUI to support the communication of encrypted commands with MXconfig/MXview.
- [MSRV-2019-006] Denial of Service by PROFINET DCE-RPC Endpoint discovery packets.
- The device would restart due to memory leak during the Nmap (a freeware that can scan the available ports) scanning test.
- RSTP Port Status error with Modbus TCP.
- Trunk port was not shown correctly in the LLDP table.
- The head switch of Turbo Chain was blocked when connecting to a Cisco switch.
- SNMP v3 memory leak.
- The device rebooted when performing a Nessus basic scan.
- MAC authentication bypass with RADIUS re-authentication.
- When SNMP pooled every 10 seconds, the system would perform a cold start after 25 minutes.
- The LLDP Table hung up in a serial console.
- Packet flooding from MGMT VLAN to redundancy port PVID VLAN.
- CERT could not be imported.
- Error with Turbo Ring v2 and port trunk LLDP display, recovery time and log miswrite.
- Relay warning did not work properly after the system rebooted.
- RSTP was not activated correctly through the configuration file import.
- Incorrect value for IGMP Query Interval on the exported configuration file.



- Logging into the web console failed if authentication with local RADIUS and account lockout were both enabled at the same time.
- Turbo Ring v2 looped when too many slaves in the ring were powered on at the same time.
- Switch automatically performed a cold start when receiving specific SNMPv3 packets.
- [CRM #200811300717] If a username had a capitalized letter then the user would not be able to log in using Menu mode.
- [CRM #190726273178] Unauthorized 802.1x devices could receive multicast and broadcast packets.
- [CRM #210115312454] Trap Server Host Name cannot be set via web GUI.
- [CRM #201019305310] Incorrect SNMPv3 msgAuthoritativeEngineBoots behavior that the value will not count up after switch reboot.
- [CRM #200702298391] The relay trigger function by port traffic overload does not work.

Changes

- The IEEE 802.1x traffic enablement method has changed from MAC-based to port-based.
- The length of the 802.1x username is increased from 32 bytes to 64 bytes.

Notes

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



Version: v6.1	Build: FWR_EDS518E_V6.
Release Date: Jan 15, 2020	

Applicable Products

EDS-518E Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- [MSRV-2017-011][CVE-2019-6561] Supports browser cookie parameters "same-site" to eliminate CSRF attacks.

Bugs Fixed

- Login issue with Chrome v65.
- The system rebooted when SNMP GET with request ID=0.
- System rebooted after SSH disconnected.
- Incorrect CPU loading was displayed.
- System rebooted when CLI "no logging" was executed.
- [MSRV-2017-006][CVE-2019-6557] Buffer overflow vulnerabilities that allowed 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 allowed users to perform XSS attacks.
- [MSRV-2017-011][CVE-2019-6561] CSRF attacks were possible if browser cookie parameters were not correct.

Changes

N/A

Notes

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



Version: v6.0	Build: 18052914
Release Date: Jan 18, 2019	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- Fixed the issue regarding obtaining information about RTSP port state errors through Modbus/TCP
- Fixed the issue that caused Loop prevent to not work when RSTP is enabled
- Fixing GUI display issue on Chrome version later than version 65.

Changes

- Support new flash and ensure it is backward compatible with the old flash
(Note: Hardware versions later than 2.0.0 only support firmware version 6.0 or later)

Notes

N/A



Version: v5.1	Build: Build_16072215
Release Date: Aug 12, 2016	

Applicable Products

EDS-518E-4GTXSFP, EDS-518E-MM-SC-4GTXSFP, EDS-518E-MM-ST-4GTXSFP, EDS-518E-SS-SC-4GTXSFP, EDS-518E-4GTXSFP-T, EDS-518E-MM-SC-4GTXSFP-T, EDS-518E-MM-ST-4GTXSFP-T, EDS-518E-SS-SC-4GTXSFP-T

Supported Operating Systems

N/A

New Features

- System Notification: Definable Successful/Failed Login notification.
- Password Policy: Password Strength can be set.
- Account Lockout Policy: Failure Threshold and Lockout Time can be set.
- Log Management: Full Log Handling.
- Remote Access Interface Enable/Disable.
- Configuration encryption with password.
- Supports SSL Certification Import.
- Supports MAC Authentication Bypass via RADIUS Authentication.
- MAC Address Access Control List or MAC Address Filtering.
- Protects against MAC Flooding Attack by MAC Address Sticky.
- NTP Authentication to prevent NTP DDoS Attack.
- Login Authentication: Support Primary & Backup Database Servers (RADIUS / TACACS+ / Local Account).
- Login Authentication via RADIUS Server: Support Challenge Handshake Authentication Protocol (CHAP) Authentication Mechanism.
- RADIUS Authentication: Support EAP-MSCHAPv2 (For Windows7).
- MXview Security View Feature Support* (with MXstudio v2.4).
- Turbo Ring v1/v2, Turbo Chain Support Port Trunking.
- Layer2 V-On support.

Enhancements

- CLI: Supports multiple sessions (up to six).
- SMTP supports Transport Layer Security (TLS) Protocol and Removes SSL v2/v3.
- SNMPv3 Traps and Informs.
- Fixed Display Issue with Java Applet.
- Fiber Check: Add Threshold Alarm.
- Static Port Lock with IVL Mode.
- Serial Number: 12 Digital S/N Display.
- When GbE Port Speed is [Auto], MDI/MDIX is [Auto] Fixed.
- Web UI/CLI Command Enhancement and Modification.

Bugs Fixed

- Drown Attack.
- ICS-VU-951212 Vulnerabilities.
- Nessus Vulnerability.

Changes

N/A

Notes

N/A



Version: v4.1	Build: Build_15022416
Release Date: N/A	

Applicable Products

EDS-518E-4GTXSFP, EDS-518E-MM-SC-4GTXSFP, EDS-518E-MM-ST-4GTXSFP, EDS-518E-SS-SC-4GTXSFP, EDS-518E-4GTXSFP-T, EDS-518E-MM-SC-4GTXSFP-T, EDS-518E-MM-ST-4GTXSFP-T, EDS-518E-SS-SC-4GTXSFP-T

Supported Operating Systems

N/A

New Features

- New release for the EDS-518E Series.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A