Firmware for EDS-G508E Series Release Notes

<table>
<thead>
<tr>
<th>Version: v6.1</th>
<th>Build: EDSG516E_V6.1_Build_20010618</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: Jan 07, 2020</td>
<td></td>
</tr>
</tbody>
</table>

### Applicable Products
EDS-G508E/G512E/G516E Series

### Supported Operating Systems
N/A

### New Features
N/A

### Enhancements
- Prevent IP base multicast control packet flooding.
- [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-2017-017] Supports HTTPS for secure communication to avoid confidential information being transmitted through clear text.
- [MSRV-2017-023] Supports configuration backup encryption mechanism to prohibit confidential information from being disclosed.

### Bugs Fixed
- Login issue with Chrome v65.
- The system rebooted when SNMP GET with request ID=0.
- The HTTP configuration was missing after the configuration file was imported.
- When DHCP remark was enabled and the VID exceeded 64, VLAN could not be added into the IGMP table.
- When DHCP remark was enabled, the VLAN tag will be added in egress.
- VLAN tag of IP/IGMP packets will be untagged abnormally.
- QoS default priority did not work.
- [MSRV-2017-003][CVE-2019-6526] Sensitive data was not encrypted.
- [MSRV-2017-009][CVE-2019-6565] No proper validation of user inputs, which allows users to perform XSS attacks.
- [MSRV-2017-010][CVE-2019-6520] Read-only user access could be superseded.
- [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-2017-014] [CWE-321] A hard-coded cryptographic key was used.
- [MSRV-2017-017] Confidential information can be transmitted using clear text.
• [MSRV-2017-023] Confidential information could be disclosed.

Changes
N/A

Notes
• MSRV is Moxa’s internal security vulnerability tracking ID.
**Applicable Products**
N/A

**Supported Operating Systems**
N/A

**New Features**
N/A

**Enhancements**
- Updated OpenSSL to version v1.0.2k.
- Increased ARP table size from 100 to 5000 entries.
- Allowed 802.1X security port to also be set as a redundancy port with all redundancy functions.
- Improved ICMP response time to be within 200 ms.

**Bugs Fixed**
- Fixed the issue that caused the device to fail when importing configuration files for different firmware to FW 5.2.
- Fixed the VLAN configuration issue on the serial console interface.
- Fixed the issue that caused the switch to duplicate IP multicast packets in disabled VLANs when IGMP Snooping was enabled.
- Fixed the issue of LLDP destination address not being correct when using trunk ports.
- Fixed Gigabit Fiber speed display issue.
- Fixed DHCP discovery fail issue.
- Fixed the issue of not being able to use Loop Prevent while RSTP is enabled.
- Fixed the link issue that occurs when the Gigabit Fiber port connects with 100M SFP and imports a configuration via CLI through that port.
- Fixed the link issue when using 100M SFP to connect with non-Moxa switches.
- Fixed the issue that causes the DHCP client to be unable to obtain an IP Address when DHCP Relay is disabled.
- Fixed the LED display error when users configure Turbo Chain to use an "even" number port as its head port.
- Fixed the looping issue that occurs when rebooting the switch using the dual homing function.

**Changes**
- Encrypted security keys in CLI commands
- Added support for new hardware version and backward compatibility with older hardware versions (Note: Hardware versions later than 2.0.0 only support firmware version 6.0 or later)

**Notes**
N/A
**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- DSCP rewrite function. This feature is only available in Command Line Interface (CLI).
- Traffic rate setting in storm protection function. This feature is only available in Command Line Interface (CLI).

Important Notice: After upgrading the firmware, please reset the switch to the factory default settings and manually input the configuration settings. Users cannot import existing configuration files into firmware v5.2 due to a change in the software design.

**Enhancements**
- Increased Access Control List (ACL) support rules from 160 to 230 rules.

**Bugs Fixed**
N/A

**Changes**
N/A

**Notes**
N/A
### Applicable Products

### 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).
- RADIUS Authentication: Support EAP-MSCHAPv2 (For Windows 7).
- MXview Security View Feature Support* (with MXstudio v2.4).
- Turbo Ring v1/v2, Turbo Chain Support Port Trunking.
- Layer 2 V-On.

### Enhancements
- CLI: Supports Multiple Sessions (up to six).
- SNMPv3 Traps and Informs.
- Fixed Display Issue with Java Applet.
- Fiber Check: Added 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
### Applicable Products

### Supported Operating Systems
N/A

### New Features
- Added new Multicast Fast Forwarding mode.

### Enhancements
- Increased IGMP Groups to 2048 (original 256 groups).
- Improved Turbo Chain link status check mechanism at the head port.

### Bugs Fixed
N/A

### Changes
N/A

### Notes
N/A
Applicable Products
EDS-G508E, EDS-G508E-T, EDS-G512E-4GSFP, EDS-G512E-4GSFP/KC, EDS-G512E-4GSFP-T,
EDS-G512E-4GSFP-T/KC, EDS-G512E-8PoE-4GSFP, EDS-G512E-8PoE-4GSFP/KC, EDS-G512E-
8PoE-4GSFP-T, EDS-G512E-8PoE-4GSFP-T/KC, EDS-G516E-4GSFP, EDS-G516E-4GSFP-T

Supported Operating Systems
N/A

New Features
N/A

Enhancements
N/A

Bugs Fixed
N/A

Changes
• Web user interface display errors under Java 8 environment.

Notes
N/A
**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- New release for the EDS-G500E Series.

**Enhancements**
N/A

**Bugs Fixed**
N/A

**Changes**
N/A

**Notes**
N/A