Firmware for EDS-408A Series Release Notes

<table>
<thead>
<tr>
<th>Version: v3.10</th>
<th>Build: EDS408A_V3.10_Build_19121910</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: Jan 06, 2020</td>
<td></td>
</tr>
</tbody>
</table>

### 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
- 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-2017-013] [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-2017-025] Supports HTTPS to ensure secure communication and stop hackers from retrieving passwords.
- [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 Javascript 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-2017-002] [CVE-2019-6563] Predictable Session ID.
• [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-2017-013] [CWE-327] Administrative credentials could be disclosed.
• [MSRV-2017-014] [CWE-321] A hard-coded cryptographic key was used.
• [MSRV-2017-016] [CWE-120] Abnormal device operations.
• [MSRV-2017-017] Confidential information can be transmitted using clear text.
• [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-2017-023] Confidential information could be disclosed.
• [MSRV-2017-026] [CWE-327] A broken or risky cryptographic algorithm was used.

Changes
N/A

Notes
• MSRV is Moxa’s internal security vulnerability tracking ID.
**Version:** v3.8  
**Build:** Build_17051216  
**Release Date:** Jun 29, 2017

<table>
<thead>
<tr>
<th>Applicable Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDS-408A-PN, EDS-408A-PN-T</td>
</tr>
</tbody>
</table>

**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
**Supported Operating Systems**

N/A

**Applicable Products**

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

**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
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
<table>
<thead>
<tr>
<th>Version: v3.1</th>
<th>Build: N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: N/A</td>
<td></td>
</tr>
</tbody>
</table>

**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