Firmware for IKS-G6824A Series Release Notes

<table>
<thead>
<tr>
<th>Version: v5.8</th>
<th>Build: 21072218</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: Sep 15, 2021</td>
<td></td>
</tr>
</tbody>
</table>

Applicable Products
N/A

Supported Operating Systems
N/A

New Features
N/A

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.

Enhancements

| 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 imported. |
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.
### Bugs Fixed

- The switch failed to recognize the SFP-1GTXRJ45-T SFP module.
- [MSRV-2017-006][CVE-2019-6557] Buffer overflow vulnerabilities that may have allowed remote control.
- [MSRV-2017-009][CVE-2019-6565] No proper validation of user inputs, which allows users to perform XSS attacks.
- [MSRV-2017-011][CVE-2019-6561] CSRF attacks were possible if browser cookie parameters were not correct.
- [MSRV-2017-012][CWE-121] A stack-based buffer overflow condition whereby the buffer that was being overwritten was allocated on the stack.

### Changes

N/A

### Notes

- MSRV is Moxa’s internal security vulnerability tracking ID.
Applicable Products
IKS-G6824A Series

Supported Operating Systems
N/A

New Features
Layer 3:
• Support tracking function.

Security Related Functions
• 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.
• Support SSL certification import.
• Support MAC authentication bypass via RADIUS authentication.
• MAC Address access control list or MAC address filtering.
• Protect 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 Windows 7).
• MXview Security View Feature Support* (with MXstudio V2.4).

Enhancements
• Web GUI supports web browser Chrome 65.0
• CLI: Supports Multiple Sessions (up to six).
• SNMPv3 Traps and Informs.
• Display Issues with Java Applet.
• Fiber Check: Add Threshold Alarm.
• Static Port Lock with VLAN filtering option.
• When GbE Port Speed is [Auto], MDI/MDIX is [Auto] Fixed.
• Web UI/CLI Command Enhancement and Modification.

Bugs Fixed
• Fix abnormal display of packet counter in the web GUI.
• When the device receives large amounts of BPDU packets on a port, the RSTP function does not enable, which might cause the device to reboot.
• If there is an ‘&’ in either the Switch Name or Switch Location column, the description will not display properly on the relevant page.

Changes
• Rate limit adds more options on the ingress rate

**Notes**

Suggestion:
• Reconfigure the device once you have upgraded to v5.x
• To ensure that the system remains stable, do not export configurations from v4.x or prior into v5.x or later
**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- Added DSCP remark function.
- Added Traceroute function.

**Enhancements**
- Encrypted all security passwords and keys in web user interface and the CLI.

**Bugs Fixed**
- VRRP did not work on RSTP ports.
- VRRP state unexpectedly changed when it took too much time to change the IGMP querier.
- VRRP state unexpectedly changed when both VRRP Fast Switchover mode is enabled and Port Trunking is set.
- Configurations could not be imported through command line, when VRRP Fast Switchover mode is set with more than 16 entries.
- Device occasionally rebooted when enabling OSPF.

**Changes**
N/A

**Notes**
N/A
Applicable Products

Supported Operating Systems
N/A

New Features
• Added new Multicast Fast Forwarding mode.
• Added new VRRP Fast Switchover mode.
• Added new Multicast Local Route.

Enhancements
• Increased IGMP Groups to 4096 (original 1000 groups).
• Improved Turbo Chain link status check mechanism at the head port.

Bugs Fixed
• Device rebooted when using CLI commands to back up device configurations to TFTP server.
• Device rebooted when using CLI commands to change SNMP v3 data encryption key and the length of key is over than 100 characters.

Changes
N/A

Notes
N/A
### Applicable Products

### Bugs Fixed
- PIM-SM multicast forwarding issues.
- Randomly hang issue when booting up.
- Topology drawing issue on MXview.
- In IGMPv3, failed to forward multicast packets on MSTP DISABLED-STATUS port.
- Failed to add Static default route (0.0.0.0/0) through the web console.
- Randomly failed to recognize Moxa SFP modules.
- In OSPF routing protocol, 10 G ports had incorrect path cost.
- Randomly failed to connect to ABC-02.
- HTTPS certification validity issue.
- There was a rebooting issue when TFTP upgraded firmware with incorrect CLI command.
- ACL CLI command failed on rules when Ether-type is 0 or IP-protocol is 0.
- Hang issue when IGMP join and leave frequently.

### Changes
N/A

### Notes
N/A
<table>
<thead>
<tr>
<th>Version: v4.0</th>
<th>Build: Build_14093015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- First release for IKS-G6824A Series.

**Enhancements**
N/A

**Bugs Fixed**
N/A

**Changes**
N/A

**Notes**
N/A