Firmware for IKS-G6524A Series Release Notes

Version: v5.8  Build: 21072618
Release Date: Sep 15, 2021

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.
- Improved random distribution of TCP Initial Sequence Number (ISN) values.

Enhancements

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.
- 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: v5.7        Build: FWR_IKSG6524A_V5.
Release Date: Feb 17, 2020

**Applicable Products**
IKS-G6524A Series

**Supported Operating Systems**
N/A

**New Features**
N/A

**Enhancements**

**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-G6524A Series

Supported Operating Systems
N/A

New Features
N/A

Enhancements
• Web GUI supports web browser Chrome 65.0

Bugs Fixed
• Fix abnormal display of packet counter on the web GUI

Changes
N/A

Notes
N/A
Supported Operating Systems

New Features
• System Notification: Definable Successful/Failed login notifications.
• 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).
• RADIUS Authentication: Support EAP-MSCHAPv2 (For Windows7).
• MXview Security View Feature Support* (with MXstudio v2.4).
• Turbo Ring v2, Turbo Chain supports Port Trunking.

Enhancements
• CLI: Support Multiple Sessions (up to six).
• SNMPv3 Traps and Informs.
• Display Issue with Java Applet.
• Fiber Check: Add Threshold Alarm.
• Static Port Lock with IVL Mode.
• When GbE Port Speed is [Auto], MDI/MDIX is [Auto] Fixed.
• Web UI/CLI Command enhancements and modifications.

Bugs Fixed
• When the device received large amounts of BPDU packets on the port that had not enabled the RSTP function, it sometimes caused the device to reboot.
• If there was an ‘&’ character in the column of the switch name, switch location, or switch description, the system info will not show on the ‘How Page’ information.

Changes
• ate limit add more option on ingress rate

Notes
N/A
<table>
<thead>
<tr>
<th>Version:</th>
<th>v4.2</th>
<th>Build:</th>
<th>Build_16112110</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date:</td>
<td>N/A</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
N/A

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

**Bugs Fixed**
N/A

**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 4096 (original 1000 groups).
• Improved Turbo Chain link status check mechanism at the head port.

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

Changes
N/A

Notes
N/A
**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- First release for IKS-G6524A Series.

**Enhancements**
N/A

**Bugs Fixed**
N/A

**Changes**
N/A

**Notes**
N/A