



## Firmware for IKS-6728A Series Release Notes

|                                   |                        |
|-----------------------------------|------------------------|
| <b>Version: v5.8</b>              | <b>Build: 21072216</b> |
| <b>Release Date: Sep 15, 2021</b> |                        |

### 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.
- Added an additional encryption option and command to the web UI and CLI.

### 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.
- The device is unreachable via web, Telnet, or ping when in a Turbo Ring topology.
- If SNMPv3 is enabled on the device, the device will reboot when importing certain configuration files through the serial console by copying the command group by group.

### **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.



|                                   |                                |
|-----------------------------------|--------------------------------|
| <b>Version: v5.7</b>              | <b>Build: FWR_IKS6700A_V5.</b> |
| <b>Release Date: Feb 04, 2020</b> |                                |

### **Applicable Products**

IKS-6728A Series

### **Supported Operating Systems**

N/A

### **New Features**

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

### **Enhancements**

N/A

### **Bugs Fixed**

- Unable to access the IM-6700A-8SFP Ethernet module after specific configurations were imported into a switch.
- [MSRV-2017-006][CVE-2019-6557] Buffer overflow vulnerabilities that may have 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 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.



|                                   |                              |
|-----------------------------------|------------------------------|
| <b>Version: v5.6</b>              | <b>Build: Build_18110817</b> |
| <b>Release Date: Jan 18, 2019</b> |                              |

**Applicable Products**

IKS-6728A-8PoE Series

**Supported Operating Systems**

N/A

**New Features**

N/A

**Enhancements**

- Web GUI support web browser Chrome 65.0

**Bugs Fixed**

- Fix the issue whereby the DHCP client was not able to obtain the IP address when the DHCP Relay is disabled
- Fix the issue that did not allow the IM module ports to be disabled
- Fix abnormal display of packet counter in web GUI

**Changes**

N/A

**Notes**

N/A



|                                   |                              |
|-----------------------------------|------------------------------|
| <b>Version: v5.4</b>              | <b>Build: Build_17080917</b> |
| <b>Release Date: Sep 04, 2017</b> |                              |

### Applicable Products

IKS-6728A-8PoE-4GTXSFP-48-48-T, IKS-6728A-8PoE-4GTXSFP-48-T, IKS-6728A-8PoE-4GTXSFP-HV-HV-T, IKS-6728A-8PoE-4GTXSFP-HV-T

### Supported Operating Systems

N/A

### 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).
- 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 v2, Turbo Chain Support Port Trunking.

### Enhancements

- CLI: Support Multiple Sessions (up to six).
- SMTP Supports Transport Layer Security (TLS) Protocol and removes SSL v2/v3.
- 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 Enhancement and Modification.

### Bugs Fixed

- Cannot receive the LLDP packet while management VID is different to PVID.
- Turbo RingV2 of Giga Copper was not stable when Profinet was enabled.
- Banner bar is not able to show special characters L <>&' "
- Port disable function of 100 SFP module was not working.

### Changes

N/A

### Notes

N/A



|                          |                              |
|--------------------------|------------------------------|
| <b>Version: v4.1</b>     | <b>Build: Build_15062316</b> |
| <b>Release Date: N/A</b> |                              |

### **Applicable Products**

IKS-6728A-8PoE-4GTXSFP-48-48-T, IKS-6728A-8PoE-4GTXSFP-48-T, IKS-6728A-8PoE-4GTXSFP-HV-HV-T, IKS-6728A-8PoE-4GTXSFP-HV-T

### **Supported Operating Systems**

N/A

### **New Features**

- Added new Multicast Fast Forwarding Mode.

### **Enhancements**

- Increase IGMP Groups to 2048 (original 256 groups)
- Backward compatible with IM-6700 Series interface modules check mechanism at the head port.

### **Bugs Fixed**

N/A

### **Changes**

N/A

### **Notes**

N/A



|                          |                              |
|--------------------------|------------------------------|
| <b>Version: v4.0</b>     | <b>Build: Build_14091014</b> |
| <b>Release Date: N/A</b> |                              |

**Applicable Products**

IKS-6728A-8PoE-4GTXSFP-48-48-T, IKS-6728A-8PoE-4GTXSFP-48-T, IKS-6728A-8PoE-4GTXSFP-HV-HV-T, IKS-6728A-8PoE-4GTXSFP-HV-T

**Supported Operating Systems**

N/A

**New Features**

- First release for IKS-6728A-8PoE.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A