



## Firmware for ICS-G7528A Series Release Notes

<b>Version: v5.10</b>	<b>Build: 23032204</b>
<b>Release Date: Apr 24, 2023</b>	

### Applicable Products

ICS-G7528A Series

### Supported Operating Systems

N/A

### New Features

- Supports the Media Redundancy Protocol (MRP).
- Supports the Secure Copy Protocol (SCP).
- Supports BPDU Guard and BPDU Filter.

### Enhancements

- The connected IGMP querier IP address can be shown in the Web interface and the command line interface.
- There is a new SNMP Trap for when the status of the Digital Input (DI) changes.
- Supports “hmac-sha2-256 & hmac-sha2-256 & diffie-hellman-group14-sha256” in SSH.
- Supports 2048-bit RSA key in SSH.
- Removed the DSA key.
- The reset button is active for 10 minutes after rebooting the device.
- The Modbus/TCP protocol is disabled by default due to security concerns.
- The SNMP protocol is disabled by default due to security concerns.
- Supports TLS v1.3.
- The SFP Enable/Disable information can be shown via the CLI.
- Supports TACACS+ Authentication, Authorization, and Accounting via the Web interface and command line interface.
- Supports resetting specific interfaces to the default parameters via the command line interface.
- Supports sequentially showing VLAN Trunk Ports with port numbers.
- Supports a new CLI command “#sh logging event-log latest” to display the event log from the newest to the oldest.
- Supports the Error Disable function for any specific ports that are linked down.
- Supports two TACACS+ servers for Authentication, Authorization, and Accounting.
- Supports SNMPv3 with AES encryption.
- Supports RADIUS logging with MS-CHAPv2 encryption.
- Displays the Web and Console management session via the Web interface, command line interface, and SNMP.
- Supports adjustable threshold settings in the Fiber Check function.
- The HTTPS Warning in Chrome and Edge browsers when importing the RootCA has been stopped.
- Reserves only two ports for Turbo Ring when the DIP switch “TURBO RING” is on. (Four ports are reserved for Turbo Ring when the DIP switch “TURBO RING” and “COUPLER” are both on.)
- Adjusts the Syslog format of Local/RADIUS/TACACS+ login for better readability.
- Supports Syslog with the CEF format.
- Related TCP ports (#502 and #44818) are disabled when disabling Modbus TCP and EtherNet/IP.
- Supports a 12-digit serial number in Modbus TCP and EtherNet/IP.

### Bugs Fixed

- When both Trap servers were set, only one of the server names could be saved.
- Operating SNMPv3 occasionally caused the device to reboot.

- Sending e-mail notifications of cold/warm events occasionally failed.
- The Gigabit port occasionally links down after configurations were restored by the ABC-02 device.
- Specific LLDP packets occasionally caused the system to perform a warm start.
- Unable to set the Trunk VLAN using MXconfig.
- Importing the configuration file failed if the offset of daylight saving is 1.
- The wording of the SNMP port type on the Web interface was UDP not TCP.
- The account and IP address of TACACS+ AAA were shown in the event log when TACACS+ AAA was successful.
- When the authorization or accounting server disconnected, the local user ID was not able to login with "TACACS+, local mode".
- VLAN configurations occasionally impacted the traffic of Trunk ports.
- When copying and pasting commands in the CLI mode, the first two syntax-rows merged, which caused an error.
- When exporting the configuration file to the TFTP server, the configuration file name included an extra backslash "\".
- Part of the packet format of GMRP was incorrect (remove "GARP\_END\_MARK").
- High latency of SSH connection and SSH key exchange.
- Communication was lost for around 300 ms when changing the VLAN setting via the CLI.
- IEEE 802.1x re-authentication could not be disabled.
- Systems that used the module SFP-1FEMLC-T occasionally flapped.
- Incorrect value was set to SNMP ifLastChange after specific interfaces were down or up.
- The system occasionally rebooted when it was set with the maximum of 64 Tagged VLANs.
- The system occasionally rebooted when the LLDP table was in a specific condition."
- The system cold started when using N-Snap login via SSH.
- Users occasionally could not connect to the system via SSH.
- [CVE-2022-0778] Import certificate issue: Update OpenSSL package.
- The event alarm was triggered on disabled ports when the event trigger alarm was set on these ports.
- [CVE-2021-27417] The unverified memory assignment can lead to arbitrary memory allocation.
- The space symbol " " in the SNMP location could not be displayed properly via the command line interface.
- The system occasionally rebooted while polling via Modbus TCP.
- System hangs or restarted when accessing the system via SSH by using Putty with version 0.60 or 0.62.

## **Changes**

- Removed "recommended browser" in the Web interface.



- Cleaned the TACACS+ and RADIUS shared keys and SNMPv3 data encryption key after changing specific configurations (TACACS+/RADIUS login list, SNMP version, SNMP auth/encrypt option).
- The default settings of "Modbus TCP Enable" was changed from enabled to disabled because of security concerns.
- The default setting of "SNMP Enable" was changed from enabled to disabled because of security concerns.

**Notes**

N/A

<b>Version: v5.8</b>	<b>Build: 21072618</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.

## 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.

### **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_ICSG7528A_V5.</b>
<b>Release Date: Feb 17, 2020</b>	

### **Applicable Products**

ICS-G7528 Series

### **Supported Operating Systems**

N/A

### **New Features**

- Supports SFP-10GLRLC-T, SFP-10GZRLC-T, SFP-10GSRLC-T, SFP-10GERLC-T SFP+ modules.

### **Enhancements**

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

### **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-2017-007][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**

- MSRV is Moxa's internal security vulnerability tracking ID.

### **Notes**

N/A



<b>Version: v5.6</b>	<b>Build: Build_18112620</b>
<b>Release Date: Jan 18, 2019</b>	

### **Applicable Products**

ICS-7528A Series

### **Supported Operating Systems**

N/A

### **New Features**

N/A

### **Enhancements**

- Web GUI support web browser Chrome 65.0

### **Bugs Fixed**

- Fix abnormal display of packet counter in web GUI

### **Changes**

N/A

### **Notes**

N/A

<b>Version: v5.4</b>	<b>Build: Build_17081010</b>
<b>Release Date: Sep 04, 2017</b>	

## Applicable Products

ICS-G7528A-20GSFP-4GTXSFP-4XG-HV-HV, ICS-G7528A-4GTXSFP-4XG-HV-HV, ICS-G7528A-8GSFP-4GTXSFP-4XG-HV-HV

## 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 supports 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

- The device received a large amount of BPDU packets on the port that did not have the RSTP function enabled, which sometimes caused the device to reboot.
- '&' character in column of switch name, switch location, switch description in system info will not show on the how page information.

## Changes

- Rate limit add more option on ingress rate.

## Notes

N/A





<b>Version: v4.2</b>	<b>Build: Build_16112110</b>
<b>Release Date: N/A</b>	

**Applicable Products**

ICS-G7528A-20GSFP-4GTXSFP-4XG-HV-HV, ICS-G7528A-4GTXSFP-4XG-HV-HV, ICS-G7528A-8GSFP-4GTXSFP-4XG-HV-HV

**Supported Operating Systems**

N/A

**New Features**

N/A

**Enhancements**

- Encrypted all security passwords and keys in web user interface and command-line interface.

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A



<b>Version: v4.1</b>	<b>Build: Build_15062312</b>
<b>Release Date: N/A</b>	

### **Applicable Products**

ICS-G7528A-20GSFP-4GTXSFP-4XG-HV-HV, ICS-G7528A-4GTXSFP-4XG-HV-HV, ICS-G7528A-8GSFP-4GTXSFP-4XG-HV-HV

### **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**

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

### **Changes**

N/A

### **Notes**

N/A



<b>Version: v4.0</b>	<b>Build: Build_14082811</b>
<b>Release Date: N/A</b>	

**Applicable Products**

ICS-G7528A-20GSFP-4GTXSFP-4XG-HV-HV, ICS-G7528A-4GTXSFP-4XG-HV-HV, ICS-G7528A-8GSFP-4GTXSFP-4XG-HV-HV

**Supported Operating Systems**

N/A

**New Features**

- First release for the ICS-G7528A Series.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A