Firmware for OnCell G4308-LTE4 Series Release Notes

Version: v3.23.0	Build: 25123121
Release Date: Jan 09, 2026	

Applicable Products

OnCell G4308-LTE4 Series

Supported Operating Systems

N/A

New Features

- Added SMTPS support in email settings.
- Added RIP routing protocol support.
- Added mechanism to detect syslog server availability.
- Added Neighbor MAC Change events.
- Added Connection Management.
- Added MXsecurity support.

Enhancements

- Added a CIP Service Code option to the EtherNet/IP (EIP) Protocol Filter Object.
- Expanded the number of bridge zones to eight sets.
- SNMP/SNMP Trap supports SHA-256 and SHA-512 authentication.
- Tech Support File allows users to generate and import files for troubleshooting.
- Ping tool supports selecting source interface.
- WAN Redundancy feature supports configuring domain names as ping hosts for each interface.
- Supports identification of embedded CIP command type (Service Code) in EIP traffic.

Bugs Fixed

- An error occurs when viewing LLDP entries through the web interface or via SSH.
- Link-up failure after device reboot.
- Failed to import configuration file.
- SNMP v3 traffic is blocked, causing devices to be SNMP-unreachable in MXview One.
- Trap information for MAC address table changes is incorrect.
- Cannot get up-to-date SNMP OID values through SNMP.
- Web interface not accessible via HTTP after HTTPS is disabled.
- System time incorrect after importing configuration.
- OpenVPN client configurations occasionally fail to import.
- Enabling GRE over IPsec sometimes causes packet loss.
- System logs frequently report unnecessary switching between Cellular WAN and 12. 12. Ethernet WAN when WAN Redundancy was enabled.
- Cellular Internet indicator occasionally red despite a successful connection.
- Incoming voice calls to device SIM number cause cellular data connection to drop.
- CVE-2025-6892, CVE-2025-6893, CVE-2025-6894, CVE-2025-6949, CVE-2025-6950 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-258121.

Changes

- Changed the behavior of user account password modification.
- When relay activates, the STATE LED also triggers.
- Cellular Diagnostics function now under “Cellular Debugging” in Diagnostic Support menu.

Notes

N/A

Version: v3.18.0	Build: 0000419725
Release Date: Jul 31, 2025	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

Added Traceroute CLI command.
Introduced multi-language support for MX-ROS, including Traditional/Simplified Chinese, Korean, and Japanese.
Added GRE interface on Network Interface.
Added OSPF support to Routing.
Added serial interface support for integration with ITS SCATS systems.
Added support for MRC Quick Link Ultra v4.1.0.

Enhancements

Added support for “Route Mode” in IPsec Startup Mode. In Route Mode, the VPN tunnel initiates only when routing packets are generated, relying on traffic to trigger the tunnel.
Added support for CLI commands to configure MXsecurity port settings.
The "Ping Response" function has been moved from the "User Interface" (MX-ROS v3.12.1 to v3.13) and "Trusted Access" (MX-ROS v3.6) pages to the dedicated "Ping Response" page.
Added IP display on the Querier Connected Port in the IGMP Snooping Group Table.
Added Passive Mode to OSPF.
Added Object types: Secure FTP and SYSLOG (TCP 514) to Object Management.
Added trap and syslog support for IPS/DPI/ADP to Advanced Protection - Configuration.
Optimized IPsec reconnection time.

Bugs Fixed

When exporting the configuration, the Object IP Range setting is saved incorrectly, causing importing the configuration to fail.
MXview 1.4.1 does not receive encrypted SNMPv3 Trap/Inform packets from the routers.
ARP Reply packets are being unintentionally dropped in Bridge mode.
Email Settings cannot be disabled.
After changing the Management VLAN, the router is unreachable when pinged.
When configuring Bridge members, the system unintentionally creates two untagged VLANs under the access port.
Multicast traffic is not filtered correctly, causing forwarding to ports that have not joined the IGMP group.
IPsec Startup Mode - Initiate Automatically does not function properly.
CVE-2024-9138, CVE-2024-9140 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-241155.
CVE-2025-0415 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-259491.
CVE-2025-0676 vulnerability issue(s). For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-251431.

Changes

Supervisor and user accounts are no longer created by default, and must be added manually. Existing accounts are not affected.
In compliance with the EU Radio Equipment Directive (RED), users must change the password on

first login.

Notes

Due to an issue, using an identical pre-shared key to set up multiple site-to-any IPsec VPN tunnels with IKEv1 mode requires a workaround. Please contact Moxa Technical Support for assistance.
Using an MRC Gateway key with a different gateway model may cause connection issues with the MRC service.