Firmware for EDR-G9010 Series Release Notes

Version: v3.14	Build: 24123112
Release Date: Dec 31, 2024	

Applicable Products

EDR-G9010 Series

Supported Operating Systems

N/A

New Features

N/A

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.

Bugs Fixed

• Routed traffic is not correctly processed according to the configured QoS rules.
• 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.
• 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.

Changes

• Changed the QoS DSCP Mapping table to start from 0x0(0) instead of 0x0(1).

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.

Version: v3.13.1	Build: 24111415
Release Date: Nov 18, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• ARP Reply packets are incorrectly dropped in Bridge Mode.
• When exporting the configuration, the Object IP Range setting is saved incorrectly, causing importing the configuration to fail.

Changes

N/A

Notes

N/A

Version: v3.13	Build: 24100800
Release Date: Oct 09, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added a CPU usage notification to Event Notification.
• Added a port usage notification to Event Notification.
• Added support for new DPI protocols to Advanced Protection: Step7 Comm+, OPC UA, MELSEC.
• Added support for RFC 5424 formatted syslog messages.
• Added a Default Action Log to Layer 3-7 Policy.
• Added support for 2.5G SFP modules.

Enhancements

• Added Syslog as a Registered Action for the VRRP State Changes event notification.
• Added syslog as a Registered Action for the Fiber Check Warnings event notification.
• Error logs for failed configuration imports now show more details.
• Users can now select multiple inbound interfaces for Static Multicast Routes within same group address.
• Added error logs for the DHCP function.
• Added error logs for the IGMP function.
• Added support for Modbus DPI protocols in the CLI.

Bugs Fixed

• The port-based DHCP server incorrectly assigns duplicate IP addresses to bridge ports.
• RSTP incorrectly assigns multiple devices as the root.
• Users are only able to configure or import one Static Multicast entry through the CLI.
• SNMP OIDs including the "newline" character returns an error.
• Importing configurations containing SNTP/NTP server or SNTP client settings results in an error.
• The NAT function does not work properly after rebooting the device.
• The PRP traffic function for MTU configuration does not work properly.
• The firewall pop-up window remains visible after the system automatically logs out.
• IEEE 802.1X authentication for the RADIUS server would fail.
• Vulnerability: CVE-2024-9137
• Vulnerability: CVE-2024-9139
• Vulnerability: CVE-2024-1086
• The connection status of the OpenVPN Client function shows incorrectly.

Changes

• Increased the maximum password and share key length to 64 characters for user accounts, IPsec, L2TP server, SNMP, IEEE 802.1X, RADIUS server, and TACACS+ server.
• Added support for special characters in passwords and shared keys for user accounts, IPsec, L2TP server, SNMP, IEEE 802.1X, RADIUS server, and TACACS+ server.

Notes

N/A

Version: v3.12.1	Build: 24082116
Release Date: Aug 26, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Unsupported or unavailable features appear in the web interface.

Changes

N/A

Notes

N/A

Version: v3.12	Build: 24073101
Release Date: Aug 02, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for the Loopback Interface function.
• Added support for the OpenVPN Client function.
• Added support for the Netflow function.
• Added support for event-triggered actions to the VRRP function.
• Added support for UDP-Flood to the DoS Policy function.
• Added SNMP Trap as a Log Destination for the Layer 2 Policy function.
• Added support for additional event log export formats: .pdf, .csv.

Enhancements

• Enhanced the following IPsec algorithms.
]Encryption: AES-256-GCM
Hash: SHA-512
DH Group: DH15 (modp3072), DH16 (modp4096), DH17 (modp6144), DH18 (modp8192), DH22 (modp1024s160), DH23 (modp2048s224), DH24 (modp2048s256), DH31 (curve25519)
PRF: PRF SHA-256, PRF SHA-384, PRF SHA-512

Bugs Fixed

• The "Login Authentication Failure Message" does not save properly.
• Using the newline character (\n) in the 'Login Message' and 'Login Authentication Failure Message' causes abnormalities in the output.
• The system is unable to ping the VRRP virtual IP.
• Users are able to bypass password policy violation warnings by pressing ESC on the keyboard.
• Time zone settings are not saved if GMT is set to 0.
• Vulnerability: CVE-2024-6387.

Changes

• Changed the IPS license expiration behavior: When the license expires, IPS functionality will now remain enabled, but the IPS patterns will no longer be updated.
• Changed the Trusted Access behavior: Trusted Access now applies to the Web UI, CLI, and New Moxa Command interfaces.
• Changed the Preempt Delay range for the VRRP function from 10 to 300 to 0 to 300.

Notes

N/A

Version: v3.6	Build: 24032802
Release Date: Apr 03, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added Turbo Chain support for Layer 2 Redundancy.

Enhancements

• Modified the DoS policy for Flood Protection to allow independent limit ranges for each interface.

Bugs Fixed

• Restoring the device configuration may fail under specific circumstances.
• The allowed characters for the Password Policy are shown incorrectly.

Changes

N/A

Notes

N/A

Version: v3.3	Build: 24010416
Release Date: Jan 12, 2024	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for TACACS+ authentication.
• Added Port Disable ingress action for Rate Limit function.
• Added support for LAN ID to DHCP option 82 in the DHCP relay agent.
• Added support for Proxy ARP for LAN interfaces.

Enhancements

• Increased maximum number of static multicast entries from 256 to 1000.
• Increased the maximum username length to 32 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
• Increased the maximum length length of passwords, communities, and shared keys to 64 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
• Unified the range of supported special characters for local account, SNMP, RADIUS, and IEEE 802.1X.

Bugs Fixed

• The STATE LED behaves abnormally when no event notifications have been triggered.
• Users are unable to access the web console if their login passwords includes "$$".
• Units are incorrectly displaying as “packets” on the vertical axis of network statistics.
• Network statistics values are inaccurate when using ports for measurement.

Changes

N/A

Notes

N/A

Version: v3.2	Build: 23100616
Release Date: Oct 13, 2023	

Applicable Products

EDR-G9010 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Enabling Bridge Mode may sometimes cause the system to perform a cold restart.

Changes

N/A

Notes

This firmware release is to address an issue originally covered in firmware version 3.0 that was not completely resolved.

Version: v3.0	Build: 23082321
Release Date: Aug 31, 2023	

Applicable Products

EDR-G9010 Series

Supported Operating Systems

N/A

New Features

• Added support for Network Security Package version 6.0 or higher.
• Added the Auto Create Source NAT setting for 1-to-1 NAT.
• Added a Range option for the 1-to- 1 NAT Destination IP Mapping Type.
• Added support for user-defined Engine ID to the SNMP function.
• Added support for SFTP to the Configuration Backup and Restore function.
• Added support for Firmware Version Checking to the Configuration Backup and Restore function.
• Added support for Password Max-life-time to the Password Policy function.
• Added support for NTP Authentication to the System Time function.
• Added support for Syslog Authentication to the Syslog function.
• Added support for Layer 2 Policy firewall logs to the Event Log function.
• Added support for DHCP Relay Agent to the DHCP server function.

Enhancements

• Compliance with the IEC 62443-4-2 industrial cybersecurity standard.
• Increased the maximum DHCP lease time from 99,999 to 527,039 minutes.
• Increased the maximum number of Zone-based Bridge interfaces from 2 to 4.
• Increased the maximum number of VLANs from 16 to 32.
• Increased the maximum number of Static Multicast Table entries from 128 to 256.

Bugs Fixed

• Enabling Bridge Mode may sometimes cause the system to perform a cold restart.
• Users are unable to change the VID of the Management VLAN.
• The SNMP encryption key incorrectly allows the use of illegal characters.
• When specifying a 64-character long IPsec pre-shared key, the system will incorrectly store it as 63 characters long.
• The SSH connection will randomly disconnect when using a non-default port configuration.
• Importing configurations will fail if Daylight Saving is enabled.
• The auto logout function of the login policy does not function properly.
• Enabling the Digital Input notification causes the STATE LED to turn red.

Changes

• Changed the HTTP port range from 1-65535 to 1024-65535 (default port: 80).
• Changed the HTTPS port range from 1-65535 to 1024-65535 (default port: 443).
• Changed the Telnet port range from 1-65535 to 1024-65535 (default port: 23).
• Changed the SSH port range from 1-65535 to 1024-65535 (default port: 22).
• Changed the maximum length of the Bridge Zone name from 13 to 12 characters.
• Removed the GOOSE Pass-through function.

Notes

• Due to changes made in this firmware release, importing the following configurations from firmware v2.0 into v3.0 will result in configuration conflicts and failure to import the configuration:
 The HTTP port number in the original configuration is set between 1 and 1023, with the exception of 80.
 The HTTPS port number in the original configuration is set between 1 and 1023, with the exception

of 443.
- The Telnet port number in the original configuration is set between 1 and 1023, with the exception of 23.
- The SSH port number in the original configuration is set between 1 and 1023, with the exception of 22.
- The length of the Bridge Zone name in the original configuration is 13 characters long.

Version: v2.1	Build: 22122916
Release Date: Jan 09, 2023	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- IPsec over L2TP behaves abnormally if IPsec settings have been configured previously.
- Static routing does not work properly after enabling dynamic routing.
- The OSPF current router ID displays incorrectly after rebooting the device.
- The Turbo Ring becomes unstable after enabling the NTP/SNTP server.

Changes

N/A

Notes

N/A

Version: v2.0.1	Build: 22101419
Release Date: Oct 20, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

- Layer 3-7 firewall policies behave abnormally after deploying the policy profile through MXsecurity.
- The system is unable to get the MXsecurity Agent Package information after booting the device.
- Users are unable to import configurations after changing the event log threshold settings.

Changes

N/A

Notes

N/A

Version: v2.0	Build: 22092310
Release Date: Sep 26, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for Intrusion Prevention System (IPS) functionality through network security packages.
• Added support for the MXsecurity management software through MXsecurity agent packages.
• Added NAT Advanced Settings.
• Added Session Control Firewall Policy settings.

Enhancements

• Updated the web user interface to the latest next-generation design.
• Layer 3-7 firewall policies are now object-based for better rule management.
• Improved firewall log categories and information layout for better readability.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v1.2	Build: 22032514
Release Date: Mar 29, 2022	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added support for built-in security packages.

Enhancements

• Increased the maximum number of static multicast routes from 32 to 256.

Bugs Fixed

• Exporting static multicast rules fails when the Static Multicast Route function is disabled.

Changes

N/A

Notes

N/A

Version: v1.1	Build: 21110913
Release Date: Dec 02, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

- Added support for the EDR-G9010 high-voltage (HV) models.
- Added support for the Turbo Ring V2 Coupling mode Layer 2 redundancy protocol.
- Added support for MSCHAPv2 authentication for RADIUS servers.

Enhancements

- Improved the phrasing of package control operation error messages.

Bugs Fixed

- CVE-2021-33909: vulnerability issue.
- The firewall and DoS event logs show incorrect information.
- Importing device configuration may fail under certain conditions.
- The local user database is invalid if RADIUS is disabled.
- The Drop Malformed Packets firewall function behaves irregularly when accessing the web UI.
- The web UI crashes when exporting the log file while the Malformed Packet function is enabled.
- HTTP would generate an error after upgrading the firmware.
- Enabling or disabling HTTPS(443) will disconnect users from the web UI.

Changes

N/A

Notes

N/A

Version: v1.0	Build: 21052417
Release Date: Jun 22, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

The first release of the EDR-G9010 series.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A