



## Firmware for EDR-8010 Series Release Notes

<b>Version:</b> v3.13	<b>Build:</b> 24100800
<b>Release Date:</b> 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.

### 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



<b>Version: v3.12.1</b>	<b>Build: 24082116</b>
<b>Release Date: Aug 26, 2024</b>	

**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



<b>Version: v3.12</b>	<b>Build: 24073101</b>
<b>Release Date: Aug 02, 2024</b>	

### 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 maximum supported number of tunnels shown at the bottom of the IPsec Settings page is incorrect.
- 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



<b>Version: v3.6</b>	<b>Build: 24032802</b>
<b>Release Date: Apr 03, 2024</b>	

**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



<b>Version: v3.3</b>	<b>Build: 24010416</b>
<b>Release Date: Jan 12, 2024</b>	

### **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 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



<b>Version: v3.1</b>	<b>Build: 23090419</b>
<b>Release Date: Sep 20, 2023</b>	

**Applicable Products**

N/A

**Supported Operating Systems**

N/A

**New Features**

- First release.

**Enhancements**

N/A

**Bugs Fixed**

N/A

**Changes**

N/A

**Notes**

N/A