Release Note for Vigor3912 Series

Firmware Version:	4.4.6.4
Release Type:	Critical – Upgrade immediately to address urgent security issues or major system risks
Applied Models:	Vigor3912, Vigor3912S

New Features

- Added a "Change Source IP" option to the Port Redirection and Open Ports rules, allowing the LAN server to see the router's LAN IP or a user-specified IP as the source address.

Improvement

Security

- Improved: Strengthened Linux kernel security by addressing 64 security issues, including CVE-2026-98432.
- Improved: Updated SQLite to address known security issues, including CVE-2025-6965 and CVE-2019-8457.
- Improved: Enhanced the security of the Web UI login page.
- Improved: Enhanced TR-069 STUN handling to address a buffer overflow issue (CVE-2024-51138) and strengthened web request handling security.
- Improved: Configuration restore now checks the file and rejects invalid content before applying it.
- Corrected: An issue where Telnet port 23 could still be reached from LAN/WAN after the Telnet port was changed.
- Corrected: An issue where the DraySOAR SSH service accepted a login before its account was created.

Reboot / Crash / Freeze / High CPU

- Corrected: An issue where the router could reboot when an IKEv2 VPN connection was disconnected.
- Corrected: An issue where the router rebooted when saving a VPN LAN-to-LAN profile with an IP address specified as the Dial-Out server.
- Corrected: An issue where the router could reboot due to the MyVigor connection.
- Corrected: An issue where the router could freeze or crash when closing USB Syslog files.
- Corrected: Possible crashes related to SNMP, Syslog, and mail alerts.
- Corrected: An issue where a long response from a customized DDNS server could cause the router to reboot.

VPN

- Corrected: An issue where L2TP over IPsec dial-in users experienced packet loss or TCP/HTTPS connection failures when accessing a LAN-to-LAN VPN.
- Corrected: An issue where IKEv2 EAP authentication failed for RADIUS users with MFA enabled.
- Corrected: An issue where L2TP VPN users authenticated through RADIUS with MFA enabled were disconnected, resulting in incorrect disconnect logs and alerts.
- Corrected: An issue where an IPsec ESP LAN-to-LAN VPN failed on a DHCP WAN when the DHCP

server and the gateway provided by different devices.
- Corrected: An issue where User-Based firewall rules were not applied to HTTP traffic from LAN to VPN.
- Corrected: An issue where the VPN server incorrectly logged scheduled-off users when an active user dialed in.

Web UI

- Corrected: An issue where Log Collector showed "Error occurred" after the login session expired.
- Corrected: An issue where the Dashboard VPN list could not show more than 8 VPN users.
- Corrected: An issue where VPN Connection Management displayed an incorrect DH group.
- Corrected: An issue where the log page of a customized DDNS profile was empty.

Others

- Improved: User-Defined DDNS profiles can now request a Let's Encrypt certificate.
- Improved: Added a firmware update reminder, shown at admin login and on HTTP web pages, when newer firmware is available.
- Corrected: An issue where new TCP connections were delayed by 30–300 ms at the start.
- Corrected: An issue where a PPPoE WAN configured for Ping Detect continued sending LCP echo requests and disconnected when no responses were received.
- Corrected: An issue where PPPoE could not dial up with some ISPs.
- Corrected: An issue where the PPPoE Server allowed only one connection per user, regardless of the Max. Login Device setting.
- Corrected: An issue where the WAN DHCP lease failed to renew when the ISP provided identical T1 and T2 timer values.
- Corrected: An issue where unresolvable hostnames in Keyword Objects generated excessive DNS queries and log entries.
- Corrected: An issue where Let's Encrypt certificate auto renewal failed due to a domain name mismatch.
- Corrected: An issue where the router checked the Let's Encrypt certificate status every few seconds when a DDNS profile had no WAN IP.
- Corrected: An issue where DDNS updates were sent repeatedly even though the WAN IP had not changed.
- Corrected: An issue where SNMP was disabled after a reboot when the Set Community field was left blank.
- Corrected: An issue where a Firewall configuration backup could not be restored on another router.
- Corrected: An issue where the Linux system could not resolve DNS names after the DNSSEC root key rollover (KSK-2024).

Known Issue

- The router may reboot repeatedly when TR-069 with XMPP is enabled. Disable XMPP to avoid this issue.

Note

- To comply with NIS2 security requirements, the firmware now applies the following defaults: Telnet is disabled, FTP is disabled, and Enforce HTTPS Access is enabled. If Telnet/ FTP access on LAN1 is unavailable after the upgrade, users are advised to verify the settings under System Maintenance >> LAN Access Control.

RD NO: 115_11_23