Release Note for Vigor3910 Series

Firmware Version:	3.9.6.3
Release Type:	Critical
Applied Models:	Vigor3910

Read First

We recommend **changing the passwords** for admin login and password/PSKs for VPN profiles after upgrading the latest router firmware (version 3.9.6.3).

Important Note

The firmware (version 3.9.6.3) has corrected a WebGUI security issue which could allow router admin and VPN credentials to be discovered if remote management was enabled without an ACL. We strongly recommend you follow the steps below to review the security settings in your Vigor router.

1. Use a strong password for admin login and all VPN profiles. Change the passwords periodically.
2. Disable any unnecessary services and VPN profiles, like OpenVPN, PPTP VPN, or remote management (Web, SNMP, telnet, SSH, FTP) from WAN. If any service is enabled, please enable ACL, 2FA, or specify the VPN peer IP to restrict the access.
3. Enable Brute Force Protection in Management setup page.
4. Record Syslog and set up VPN/login Mail Alerts and review the logs periodically. While seeing the abnormal attack events, we can enable DoS Defense and block those IPs by using the Blacklist.

Improvement

- Improved: Improve the WebGUI security.

Known Issue

- Once upgraded to 3.9.2.2, configuring route policy settings and then get downgraded to 3.9.2.1 or older, route policy “to” and “failover” to settings are likely to be wrong. Always backup your config before firmware up(down)grading.
- Once upgraded to 3.9.2.x, configure IP Bind MAC settings and then get downgraded to 3.9.1 again. The IP Bind MAC settings will disappear. So make sure the IP Bind MAC settings is backed up before downgrading.