NO:AP1101-2 V.1

Release Note for Vigor2762 Series

Firmware Version:	3.8.8.2
Release Type:	Critical
Applied Models:	Vigor2762, Vigor2762n, Vigor2762ac, Vigor2762Vac

Vigor2762 series, the high speed router, are perfectly complied with VDSL2 environment including Vigor2762n and Vigor2762ac for speed-wanted customers. With high throughput performance and secured broadband connectivity provided by Vigor2762 series, you can simultaneously engage these bandwidth-intensive applications, such as high-definition video streaming, online gaming, and Internet telephony / access.

This is a critical update - You should upgrade such Vigor router immediately with firmware containing these improvements.

File and Modem Code

Note: For DSL models, there will be two folders: STD and VECTOR. The files in VECTOR folder implement a new DSL driver, which supports G.Vectoring on VDSL. If you're using a VDSL line, VECTOR firmware may brings out better performance; however, please consult your ISP to check if G.Vectoring is required. We also provide several versions of Vector firmware to avoid the interoperability issue. You could just try the other one if the one you use cannot synchronize or get the speed that you expected.

Available modem codes for Annex A/Annex B are displayed as follows:

For Annex A Model,

- "Vigor2762_v3.8.8.2_STD.zip" is used for modem code 776d07_772801 & 774307_771801
- "Vigor2762_v3.8.8.2_VECTOR1.zip" is used for modem code 779517_773F01 & 776d07_772801.
- "Vigor2762_v3.8.8.2_VECTOR2.zip" is used for modem code 77B506_775401 & 776d07_772801.

For Annex B Model,

- "Vigor2762_v3.8.8.2_STD.zip" is used for modem code 773306_771502 & 773307_771C02.
- "Vigor2762_v3.8.8.2_VECTOR1.zip" is used for modem code 773306_771502 & 773307_771C02.
- "Vigor2762_v3.8.8.2_VECTOR2.zip" is used for modem code 773306_771502 &

773307_771C02.

New Features

- None.

Improvement

- This firmware includes improvements to harden the web interface against attacks. We have become aware of specific attacks against router, including DrayTek models where hackers have altered specific settings relating to your DNS servers and DHCP settings. You should urgently check those settings on your router. If they appear to have been tampered with, correct them and change your admin password and for any other config anomalies. Restore a config backup if you have one (from prior to the attack). We continue to investigate this issue but the first priority was to issue updated firmware.

Known Issue

- None.