Gen2 (“RuggedVPN”) Firmware Release 2024043070 /2026052550 for Viprinet and Wantastic products; June 2026

The focus of this firmware release is improving resilancy of VPN Hub models against DDoS attacks and TLS exploit scans. While we also have hardened some security parameters, this is mostly about preventing exploit scans and bots to eat up system resources, slowing VPN Hubs down.

In addition to this a couple of small fixes have been implemented.

This is the final release for all old products that had been declared as Out of Service. For further information, please consult our Firmware support matrix.

Important pre-installation instructions:

- **This firmware release does not apply to Hub 5020 products. For these, a new firmware generation (Gen3) release will become available in early July 2026.**

- **Protect the Elderly:** Very old routers (10+ years), especially units that have been operated at sub-optimal temperature ranges often will have a faulty/very aged flash memory, and sometimes drained batteries or capacitors. Quite often they still work absolutely normally, but as soon as the flash is written with the new firmware, they fail. For those old routers installing this firmware update may cause the flash to finally die, with the router no longer starting.

  Therefore when updating very old routers, please take extra care. Make sure you have taken a configuration backup, and have a replacement device in case something goes wrong.

- This firmware release is backward-compatible to old releases, including the ones from back in 2018. This means you can first upgrade the Hub, and then upgrade the Node router at a later point. Please note however that all performance enhancements will only be seen once both sides are updated.

Changes compared to the July 2024 (2024043070/2024070250, For Hub 5020: 2024052290/2024070200) Release

Improvements

- VPN Hubs are now far more resiliant against TCP SYN flood attacks.
- Various improvements to the TCP TLS implementation for the Web Interface and VPN Tunnels. While this only makes a marginal improvement on real-life system security, it will give a much better score for our systems when doing compliance audit scans.
- Added support for the upcoming “4.5G Global LTE Cat.6” hot-plug module.
- We have updated the store of trusted TLS CA certificates. This is relevant for example when using our HTTP download tool, so that HTTPS certificates from now Certificates Authorities are accepted.
- Added End-of-Service banner for relevant products with a link to a page that will give further instructions which hardware upgrade options exist.
- Added rule for HTTP QUIC (UDP Port 443), Webex Cloud to the QoS templates, also increased minimum bandwidth for voip. Please note that your existing QoS templates will not be overwritten, if you wish to use those changes you first have to use the “Restore QoS templates to factory defaults” function, and then apply those templates to the VPN Tunnels you wish to use those settings in.

Bug fixes

- Fixed rare internal error 2323A23BC2919129 which could be caused due to channel write buffers running over. The error caused a channel disconnect, which now no longer happens, instead that issue is clearly recovered
- Fixed a rate bug where in case a flow with a VLAN tag was found NAT could fail. This could have resulted in all kinds of weird problems when using tunnel segmentation.
- In case of issues with an Ethernet LAN or WAN NIC, in most cases these will now cleanly be recovered from.