Release Notes for DrayTek Vigor2866 series (UK/Ireland)

Firmware Version	4.4.5.2_BT (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	31st July 2024
Release Date	13th August 2024
Revision	5263_fa7be4b901
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Web GUI security improvements

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading
2. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:

```
ppa -E -e 1
ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
```

Notes

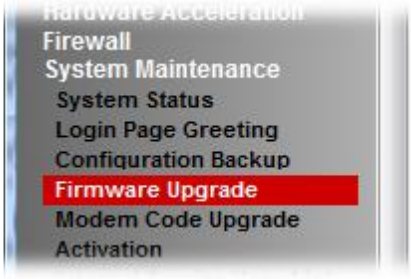
1. IPsec HMAC (MD5) is no longer supported

Firmware File Types

The ZIP file contains the firmware with two different file extensions, .ALL and .RST. The firmware is identical, but the RST file contains factory default settings. If you install the ALL file, your router will retain all existing settings. If you use the RST file, all settings will be wiped from your router.

Upgrade Instructions

It is recommended that you take a configuration backup prior to upgrading the firmware. This can be done from the router's system maintenance menu.



To upgrade firmware, select *'firmware upgrade'* from the router's system maintenance menu and select the correct file. Ensure that you select the ALL file unless you want to wipe out your router's settings back to factory default.

Manual Upgrade

If you cannot access the router's menu, you can put the router into 'TFTP' mode by holding the RESET whilst turning the unit on and then use the Firmware Utility. That will enable TFTP mode. TFTP mode is indicated by all LEDs flashing. This mode will also be automatically enabled by the router if there is a firmware/settings abnormality. Upgrading from the web interface is easier and recommended – this manual mode is only needed if the web interface is inaccessible.

Firmware Version	4.4.5.1_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	19th April 2024
Release Date	27th June 2024
Revision	5254_a83bf0bb58
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Password mechanism changed to force admin to change the password from the default password

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading
2. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:
   ```
   ppa -E -e 1
   ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
   ```

Notes

1. IPsec HMAC (MD5) is no longer supported

Firmware Version	4.4.5_BT (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	26th March 2024
Release Date	18th June 2024
Revision	5249_1c62d40892
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

1. PPPoE WAN mode supports MTU auto negotiation

Improvements

1. The Auto APN parameter can be disabled via VigorACS (TR069)
2. Discord added to [CSM] > [App Enforcement]
3. [VPN and Remote Access] > [VPN Matcher] can select WAN interface
4. Web GUI security improvements (CVE-2024-23721)
5. LTE OID added for RSCP
6. A new service provider added: SMSala
7. Additional information can be displayed via Webhook
8. The active SIM card can be displayed in the [LTE] > [Status] page
9. Visual improvements to the Router Summary section on the login page
10. SIM1/2 ICCID can be displayed when the SIM is disabled in the settings of the router
11. Enabling SNMP does not require a reboot of the router
12. Fix for the Hotspot Web Portal loop
13. Improvements to the SMS object profile mechanism
14. Obtaining all TR-069 parameters via SSH did not work
15. Fix for the IPsec VPN traffic not working when connecting using IKEv2
16. The MyVigor page could not be opened via Product Registration
17. Fix for the failure to show WAN IP information on CPE Notify page
18. Fix for the failure with menu options displayed for Diagnostic user on router login
19. Redirection to the login page in User-Based mode could take longer than expected
20. In some circumstances DNS requests could not be resolved
21. Customer's logo could not be properly displayed on the router's login page
22. WCF/DNSF didn't work when the domain name exceeded 63 characters
23. The router could stop responding when airplay was used by connected wireless devices
24. The router did not apply a static IP for remote dial-in VPN profiles if the selected interface was part of a router LAN
25. In some circumstances OpenVPN tunnel could not be established
26. The VPN traffic would continue via the failover WAN interface even when the primary WAN had been restored
27. Rebooting the router could fail when VigorACS CPE set parameter configuration contained WAN1 username/password
28. The CPE could sent the wrong '1 BOOT' event (instead of '0 BOOTSTRAP') to VigorACS after executing factory reset

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading
2. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:
   ```
   ppa -E -e 1
   ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
   ```

Notes

1. IPsec HMAC (MD5) is no longer supported

Firmware Version	4.4.3.2_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	6th December 2023
Release Date	29th January 2024
Revision	4711_9ff141f54a
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Router-based Central AP Management is compatible with VigorAP 1062C
2. Improvements to the LTE connection
3. Web GUI security improvements (CVE-2023-47254)
4. IPsec phase 2 network ID can be displayed on the router's dashboard
5. Ping Diagnosis did not work with route policy
6. IP objects could not be displayed on VigorACS server
7. WCF URL Reputation Queries could timeout when over 64 bytes-long domains were checked

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading.
2. QoS does not work on G.fast line when the link rate exceeds 600 Mbps
3. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:
   ```
   ppa -E -e 1
   ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
   ```
4. Data Flow Monitor shows NaN output while Bandwidth Management is enabled

Firmware Version	4.4.3.1_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	6th October 2023
Release Date	2nd November 2023
Revision	4694_c90a9d3b99
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Bind IP to MAC can replace or add new devices for specific period of time
2. Fix an issue with WAN2 L2TP
3. Improvements to the IPSec multiple SA using phase2 network ID function
4. The router could stop responding while using LTE module for a long time
5. Fix an issue where the VPN tunnel between the VPN server (Vigor router) and a client could not be disconnected
6. The issue where Central AP Management profiles could not be applied to access points has been resolved
7. As a prevention measure against XSS, login page logo pictures can no longer be externally hosted. They must be uploaded to router via [System Maintenance] > [Login Page Greeting]

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading.
2. QoS does not work on G.fast line when the link rate exceeds 600 Mbps
3. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:
   ```
   ppa -E -e 1
   ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
   ```
4. Data Flow Monitor shows NaN output while Bandwidth Management is enabled

Firmware Version	4.4.3_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	11th July 2023
Release Date	18th August 2023
Revision	4640_0874248bce
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

1. Support for the new WCF provider – URL Reputation. If you have an existing activate licence, then this will be upgraded to the URL Reputation licence
2. Support for WireGuard VPN

Improvements

1. VPN interface can be selected for [NAT] > [Open Port] configuration
2. Support for HTTP compression to reduce the TR-069 payload size
3. User access to CPE can be authenticated by external Radius server
4. Web GUI security improvements
5. Additional SMS commands are now supported (set and get TR-069 parameters), e.g.
   ```
   tr069 get "TR069 parameter" "password"
   tr069 get InternetGatewayDevice.LANDevice.1.WLANConfiguration.1.SSID
   1234
   ```
6. Support for more LTE SNMP OIDs
7. Improved Bind IP to MAC security
8. Improvements to Auto APN settings for Gamma SIMs
9. Improvements to SIM1/SIM2 failover mechanism
10. System statistics can be displayed on the login page
11. Support for writable/read-only TR-069 parameters notes
12. Fixed the Bridge VLAN over mesh network connectivity
13. In some circumstances the DHCP relay did not work
14. Fixed an issue with error message of HTTP Content Error that would appeared while trying to import ovpn (OpenVPN) file
15. The Smart VPN Client 2FA window did not appear when using IKEv2 EAP and any router LAN IP address except the first one
16. When OpenVPN to Pfsense was established, the push route from the server could not be completed
17. Fixed an issue with the key data loss for OpenVPN client config file when exported from VigorACS
18. In some circumstances graphs displayed on the VigorACS page would show gaps
19. An individual SIM slot can be enabled/disabled
20. Incorrect data was shown on WUI when SIM budget was enabled
21. Fixed an issue related to authentication on External Hotspot Server and the External RADIUS Server
22. The WPS button would not enable nor disable the wireless bands

23. Improvements to the issue with empty .json response for CPE when using VigorACS API
24. The Let's Encrypt certificate could not be renewed automatically
25. Fixed an issue that could result in 'Firmware Damage' being reported when upgrading from VigorACS
26. The Firmware Damage state would remain after uploading the wrong file (file size 0)
27. Fixed the DNS PTP records
28. The router could stop responding when L2TP with IPsec (LAN to LAN) VPN profile was created
29. The router could stop responding when IKEv2 re-dialed and the local ID was set to 32 characters
30. Some configuration backup files from 2862 models could cause the router unresponsive
31. The router did become inactive after WAN IPv6 was renew

Known Issues

1. A firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. The router's firewall block rules can stop remote management and VPN access. It is recommended to review the firewall settings before upgrading.
2. QoS does not work on G.fast line when the link rate exceeds 600 Mbps
3. For "ax" series model:
   Some wireless clients might encounter unexpected trouble (e.g., unable to use the printer on LAN) while accessing the Internet if the hardware acceleration is enabled.
   To skip hardware acceleration for certain devices, the following telnet command can be used:
   ```
   ppa -E -e 1
   ppa -E -a AA:BB:CC:XX:XX:XX nat|bridge|ipsec
   ```
4. Central AP Management profiles can't be applied to specific access points. Use provisioning option as a temporary workaround

Firmware Version	4.4.2_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	23rd February 2023
Release Date	22nd March 2023
Revision	4087_45783803c5
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

1. TOTP 2-factor authentication (Google Authenticator) is now available for authenticating Remote Dial-In User VPN connections
2. The Vigor2866ax model can act as Mesh Root (With VigorAP 906 nodes only)

Improvements

1. The TR-069 traffic can be sent over IPv6
2. Support for AES-GCM algorithm for IPsec/L2TP Dial-In connections
3. Improved the mesh network stability
4. The PKC12 certificate chain files are now supported
5. Static route sessions can be processed by hardware acceleration
6. Increased number of characters to 128 characters for APM and SWM password length
7. Mesh Root TCP port 9608 could be detected on WAN when enabled
8. Dynamic DNS (DrayDDNS profiles) can be set in round robin or WANx First configuration
9. Wireless WAN can automatically switch to another channel
10. The default SSID name for 2.4GHz/5GHz bands has changed to the following syntax:
    DrayTek-xxxxxx / DrayTek5G-xxxxxx
    where "xxxxxx" are the last 6 digits of the product's MAC address
11. Routers could not connect to GenieACS servers
12. SNMP OID could not display VPN status
13. Improvements to the WPA Enterprise security mechanism
14. Fixed an issue where an incorrect DNS server would answer queries when the router was set as the DNS server
15. In some circumstanced a policy route would stop working when hardware accelerated was enabled
16. When changing the IP address into 0.0.0.0/0 for the "Create a unique SA for each subnet(IPsec)" option (VPN profile #2), the configuration would not be saved properly
17. The firewall default rule would block the L2TP traffic (WAN to Localhost)
18. When OpenVPN default gateway option is disabled [VPN and Remote Access] > [OpenVPN] > [Client Config], Windows OpenVPN client could still send DNS requests via the VPN tunnel
19. Fixed an issue where only five Remote Dial-In User profiles could be restored if they were saved on other routers
20. OpenVPN Windows users could no access router's LAN (when using the WAN2 / LTE interface)
21. The TR-069 SDWAN data could not be displayed on the Vigor ACS server due to a wrong format of the Authorization URI in the Bulkdata packet (too many "/" characters)

22. The router would not display no response messages when a failed connection to the secondary TR-069 server occurred via WAN2 interface
23. IPsec HMAC (MD5) is no longer supported

Known Issues

(None)

Firmware Version	4.4.1.1_BT (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	10th January 2023
Release Date	3rd March 2023
Revision	3023_4045389c8
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improvements to the Web GUI Security (CVE-2023-23313)

Known Issues

(None)

Firmware Version	4.4.1_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	21st June 2022
Release Date	29th July 2022
Revision	3022_cb1ba35e8
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improved memory management mechanisms

Known Issues

(None)

Firmware Version	4.4.0_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	12th May 2022
Release Date	24th June 2022
Revision	3019_f8fc132a7
Applicable Models	Vigor2866, Vigor2866ac, Vigor2866ax, Vigor 2866Lac, Vigor2866Vac
DSL Modem Code	1232305
Locale	UK & Ireland Only

READ BEFORE UPGRADING!

This firmware alters the firewall behaviour.

The firewall is now able to block inbound requests to the routers management and services interfaces such as the Web UI and VPN Services. The firewall treats these as [WAN to LocalHost] for direction purposes.

If your [Firewall] > [General Setup] > Default Rule is set to Block, you must set it to Pass before upgrading the firmware.

If you want to set the default rule to block, then after upgrade, create pass rules with a direction to [WAN to LocalHost] so that the Web UI (typically TCP 443) is exempt by creating a Pass rule first. Other common services used by the router are:

HTTPS & SSL VPN	-	TCP 443
SSH	-	TCP 22
IPSEC	-	UDP 500
IPSEC NAT-traversal	-	UDP 4500

New Features

1. Firewall can restrict/drop unwanted inbound WAN traffic such as VPN requests. Use the new direction option **[WAN -> Localhost]** to apply
2. Router's DNS server feature can record one domain with multiple IP addresses
3. Support for Link Aggregation (LAG) for selected LAN ports
4. [Certificate Management] system now operates in a new way:
    a) HTTPS certificate for management & SSL VPN is now selected from:
    [Certificate Management] > [Local Services List]
    Reboot the router after changing this setting to use the new certificate
    b) [Local Certificates] now supports more than 3 certificates
    c) [Trusted CA Certificates] now supports more than 3 certificates
    d) Storage for Certificate on each of those pages shows % remaining available space
    e) Password on Private Key is no longer required when importing Cert + Private Key
5. Inbound QoS now supports Hardware Accelerated operation
6. Support for network monitoring protocol IPFIX (Netflow)
7. SNMP 'ifLastChange' is now supported for WAN and LAN port uptime (Physical port link up/down detection)

8. App-level Bandwidth Limits (e.g. Teams, OneDrive, Steam) can now be configured from [Bandwidth Management] > [Bandwidth Limit] > [APP]
9. Webhook feature can now be enabled in [System Maintenance] > [Webhook] to send periodic keepalive / heartbeat messages to a monitoring server
10. Cache password for auto reconnect option added on the [VPN and Remote Access] > [OpenVPN] > [Client Config] page
11. Wake on LAN via WAN can now be enabled/disabled for allowed IPs or any WAN IP from [Applications] > [Wake on LAN/WAN] – Wake on WAN tab

Improvements

1. Improved Web GUI Security
2. Updated HTTPS mechanism to address the CVE-2022-0778 (OpenSSL)
3. Support for IKEv2 fragmentation to improve IKEv2 EAP compatibility
4. Hardware Acceleration is enabled by default when router is reset or upgraded with .rst file
5. DNS Filter now supports blocking of DoH (DNS over HTTPS) and DoT (DNS over TLS) services to ensure that users use standard DNS, allowing the DNS Filter to operate optimally
6. Exception list added to [Hardware Acceleration]
7. Updated encryption mechanism for MyVigor server connections for license obtaining, network connecting, and registrations
8. Improved NAT performance for Hotspot Web Portal with asynchronous mode
9. When Brute Force Protection is disabled, service options are greyed out (ticked by default)
10. Syslog improvements for attempted OpenVPN connections
11. Function priority and default value change for DoS & Bandwidth Limit and HW NAT settings
12. In some circumstances Conditional DNS Forwarding did not work
13. Improved mesh network connectivity
14. Fixed a display issue with Basic Configuration Sync in the Mesh setup section
15. Self-sign certificate renewal mechanism improvements related to DrayDDNS Let's Encrypt
16. PPTP VPN users could not access router's WUI
17. In some circumstances Port Redirection did not work when Hardware Acceleration for NAT and 802.1Q priority for LAN were enabled
18. Disabling a static route could disable the default route entry
19. When default modem code was used, router would not connect to ADSL
20. After the firmware upgrade, router could stop responding if VoIP call, and VLAN configuration were in use
21. Self-signed certificate will now automatically regenerate before expiring
22. Some wireless clients could not reconnect to 2.4 and 5GHz
23. Customized List data information display issue fixed for [LAN] > [General Setup], DHCP Server Option section

Known Issues

(None)

Firmware Version	4.3.2.1_BT (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	25th October 2021
Release Date	11th November 2021
Revision	11161_2109_a730b4f5e1
Applicable Models	Vigor2866, Vigor2866ac, Vigor 2866Lac
DSL Modem Code	1232305
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Self-signed certificate will automatically regenerate before expiration
2. System stability improvements
3. Hardware Acceleration did not work with WAN to LAN sessions in routing mode

Known Issues

(None)

Firmware Version	4.3.2_BT (Formal Release)
Release Type	**Initial Release**
Build Date	22nd June 2021
Release Date	18th July 2021
Revision	8731_2104_b0731bb564
Applicable Models	Vigor2866, Vigor2866ac, Vigor 2866Lac
DSL Modem Code	1232305
Locale	UK & Ireland Only

First Firmware Release for this model

New Features

(None)

Improvements

(None)

Known Issues

(None)

[END OF FILE]