Release Notes for DrayTek Vigor 2926 series (UK/Ireland)

Firmware Version	3.8.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	16th July 2018
Release Date	10th August 2018
Revision	75315
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Firewall filter rules were not correctly applied to Routed LAN subnets
2. Improved interoperability with Hotspot Web Portal and Facebook authentication service
3. Web interface could not be accessed via HTTPS from in some network environments
4. A new Self-signed certificate could not be generated from [System Maintenance] > [Self-Signed Certificate] > Regenerate
5. NAT loopback could not operate with port forwards configured using ports 768 to 1023
6. Wireless clients connecting to 2.4GHz wireless SSID and disconnecting could not connect to 5GHz wireless SSID, receiving an invalid security key error
7. Entering a speech mark character i.e. " in the Pre-Shared Key for wireless SSID 2, 3 or 4 would result in the wireless security settings for SSID 2, 3 and 4 being inaccessible from the web interface
8. The "Analyse a single packet" mode of [Diagnostics] > [Route Policy Diagnosis] could not be displayed correctly in Google Chrome browser

Known Issues

1. The IP Filter does not apply to traffic using [Routing] > [Static Routes] in firmware 3.8.9 and later.
2. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.
   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2] by changing the Enable setting of WAN2 to "Set as LAN".

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	3.8.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.8.2) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.8.2.
Build Date	12th June 2018
Release Date	9th July 2018
Revision	74522
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

Security Advisory

1. Check your DNS and DHCP settings on your router.
   https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks
   If you have a router supporting multiple LAN subnets, check settings for each subnet. Your DNS settings should be either blank, set to the correct DNS server addresses from your ISP or DNS server addresses of a server which you have deliberately set (e.g. Google 8.8.8.8). A known rogue DNS server is 38.134.121.95 - if you see that, your router has been changed.

New Features

1. WAN2 (Ethernet) port can now operate as a LAN port when disabled in [WAN] > [General Setup] > [WAN2], for a total of 5 LAN ports, by selecting "No-Set as LAN" as the Enable option
2. Firewall Filter rules can now be linked to specified LAN and WAN interfaces by selecting a Direction then clicking Advanced and selecting the interfaces that the Filter rule will affect
3. ISO 3166 Country objects configured in [Objects Setting] > [Country Object] menu can be applied as Source / Destination IP ranges in Firewall Filter rules
4. LAN IP Alias added to [LAN] > [General Setup] to define which WAN is used for outbound traffic by sending to a different Gateway address for the router
5. Support DrayOS IKEv1 IPsec XAuth as a VPN protocol for Remote Dial-In User VPN tunnels
6. Support for EAP Tunnelled Transport Layer Security (EAP_TTLS) security method added to [Applications] > [Local 802.1X General Setup].
7. Configuration backup / restore is now available for Remote Dial-In User and LAN-to-LAN profiles to back up all VPN profiles configured, separately from the main router configuration file
8. Larger certificate files now supported in [Certificate Management] > [Local Certificate] making it possible to include additional certificates required to complete a certificate chain
9. Support for mOTP and 2FA (two factor authentication) via e-mail/SMS added for remote management in [System Maintenance] > [Administrator Password]
10. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected

Improvements

1. Fixed the App Enforcement profile issue in 3.8.9 firmware
2. Fixed the Web UI Issue if Bandwidth Limit and Data Flow Monitor were enabled in 3.8.9 firmware
3. Support for VigorACS 2 version 2.3.0
4. Improved device compatibility with router's 5GHz WLAN and AES encryption
5. Layout of [WAN] > [Internet Access] > [Details Page] improved to group essential settings in the left pane, with additional / advanced options grouped in the right pane
6. Subnet Mask settings in the web interface now use a drop-down box for selection
7. The number of characters allowed in a text box, such as a username or password field, is now displayed in the web interface when no text is entered in that text box
8. Layout of [VPN and Remote Access] > [Connection Management] improved with separate tabs for active LAN-to-LAN and Remote Dial-In User VPN tunnels
9. Layout of [Bandwidth Management] > [Quality of Service] improved
10. DoS Defence moved to [Firewall] > [Defence Setup]
11. Anti-Spoofing Defence settings for IP and ARP spoofing added to [Firewall] > [Defence Setup]
12. Certificate import can now be performed via CLI using "mngt cert_import" command via URL
13. Removed deprecated CLI commands "ip dmz" and "ip aux [Join to NAT pool]"
14. Added "IPv6 Address Random Allocation" option for DHCPv6 Server settings
15. IKEv2 LAN to LAN VPN tunnels can specify these new Proposal options:
    a. Diffie-Hellman (DH) Group 19 (256-bit Elliptic Curve)
    b. Diffie-Hellman (DH) Group 20 (384-bit Elliptic Curve)
    c. Diffie-Hellman (DH) Group 21 (512-bit Elliptic Curve)
16. The Router Name set in [System Maintenance] > [Management] can be used as L2TP Client's Host name
17. Central AP Management profiles now have options to configure AP-assisted Client Roaming parameters
18. Support Channel Width selection on [Central Management] > [AP] > [WLAN Profile]
19. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected
20. Improvements to WAN Budget scheduling
21. Inter-LAN Routing table in [LAN] > [General Setup] now allows routing between LAN1 and DMZ when VLANs are not enabled
22. Improved load balancing algorithm for VoIP – STUN and SIP connections will now remain on the same WAN interface by default
23. Session timeout values for SSH and Telnet can now be adjusted with "mngt telnettimeout/sshtimeout" CLI commands
24. Improved Bandwidth Limit operation when used in conjunction with QoS
25. If TR-069 was configured with STUN, the resulting UDP connection request address would still be sent to the TR-069 server after disabling STUN for TR-069
26. Unable to pass traffic through VPN when VPN Trunk Backup connection was resumed
27. The web interface did not accept IPv6 Object IP addresses ending with "::"
28. Improved warning notifications given when disabling LAN ports, USB ports, LEDs and buttons in [System Maintenance] > [Panel Control]

29. Syslog incorrectly displayed the password setting for WAN DHCP Client Identifier
30. The router could sent incorrect DNS queries if Syslog / Mail Alert was enabled
31. Improved VLAN Tag Insertion layout for [WAN] > [General Setup]
32. Schedule entries are now selected from a drop-down box which displays each schedule entry number and configured Comment fields
33. Schedule entries configured to operate overnight did not work correctly
34. Improved handling of Firewall filter rules configured to operate on a schedule
35. Enabling Session Limit could block Internet connectivity for Remote Dial-In User VPN tunnel connections from VPN clients sending Internet traffic through the VPN tunnel
36. NAT Port Redirection entries configured through the CLI did not take effect unless disabled and re-enabled
37. NAT Port Redirection entries configured with TCP protocol could not be enabled
38. Improved USB storage handling, to better handle USB storage being unplugged while reading data from the USB for a user connected to the router's FTP server
39. Improved interoperability of the DHCP Relay function with Windows Server's DHCP server
40. DHCP Relay did not work with Remote Dial-In User VPN tunnels
41. Enabling "Allow management from the Internet" option for IPv4 could also enable this option for IPv6 Internet connections
42. Entering a Pre-Shared Key(PSK) containing " in [Wireless LAN] > [Security] would cause that settings page to display incorrectly
43. [Central AP Management] > [WLAN Profile] could not set TX Power for 5GHz WLAN
44. USB Disk could not be detected upon reconnection after disconnecting via WUI
45. Improved compatibility with "freedns.afraid.org" and "UBDDNS" Dynamic DNS providers
46. Log information could not be displayed for DtDNS Dynamic DNS hostname updates
47. The Domain Name "ddns.net" could not be selected when using No-IP.com Dynamic DNS
48. Added support for EntryDDNS Dynamic DNS provider
49. Unable to get DrayDDNS domain name after registering and activating the DrayDDNS license
50. TR-069 Packet Counters for LAN ports could still increment when the port was not in use
51. The "Don't Fragment" flag of an IP header was not processed correctly in all scenarios
52. Could not register Avaya phone [H.323] to IPPBX server through router's NAT
53. Multiple objects can now be selected configuring an object group
54. Added "Next" and "Previous" links on each object profile editing page
55. DHCP Broadcast packets from LAN clients could incorrectly be sent out through the WAN2 interface in some circumstances, affecting WAN2 connections using DHCP for IP allocation
56. DHCP server state of LAN Subnets could be displayed incorrectly on the [Dashboard]
57. Auto VoIP QoS is now applied to routed LAN subnets
58. Wireless clients could not communicate with wired clients in the same VLAN with a VLAN tag
59. Incoming RDP sessions cannot authenticate with Firewall configured for User-based mode
60. QoS LED could be incorrectly lit if QoS was enabled then disabled
61. Restart is no longer required for changes to [Applications] > [RADIUS/TACACS+] > [Internal Server] when enabling/disabling Internal Radius Server or modifying the Authentication List
62. Remote Dial-In User VPN connections could not access the Internet through the VPN tunnel if Hardware Acceleration was enabled on the router
63. Some IPv6 packets were incorrectly blocked by the IP Filter with rules configured to pass these IPv6 packets

64. Resolved display issue with Bind IP to MAC enable/disable setting in VigorACS 2
65. When the Interface - LAN section is expanded on the [Dashboard], click on Host ID/Comment text to switch between ARP Table's Host ID and Bind IP to MAC's Comment
66. Added switching between viewing All Users and Online Users view in [User Management] > [User Online Status] by clicking on the text in the upper right
67. Bind IP to MAC was incorrectly limited to 300 entries instead of 1024
68. Increased Hotspot Web Portal profile Terms and Conditions Content field length to 1360 characters
69. Idle timeout value was not applied to Remote Dial-In User tunnels using SSL VPN
70. ARP Table displayed Comments incorrectly for some IP addresses i.e. x.x.x.10 would display the same comment as x.x.x.101
71. "CN" and "cn" values (Common Name Identifier) for LDAP now operate in the same way
72. PPPoE status messages were not displayed in [Physical Connection] > [Online Status]

Known Issues

(None)

Firmware Version	3.8.9 (Not Released)
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.8.2) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.8.2.
Build Date	21st May 2018
Release Date	-
Revision	73984
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

(See Firmware 3.8.9.1)

Improvements

(See Firmware 3.8.9.1)

Known Issues

1. **Important Note – WAN2 Factory Default configuration:**
   The WAN2/LAN5 port is set to operate as the WAN2 port by default.

   To use this port as LAN5, it must be configured in [WAN] > [General Setup] > [WAN2].
   Set the Enable setting of WAN2 to "Set as LAN" and click OK. The WAN2/LAN5 port will operate as LAN5 once it has restarted.

2. The router cannot be managed from the Web UI if Bandwidth Limit is enabled on the router. This will be corrected in the next firmware release.

Firmware Version	3.8.8.2 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	18th May 2018
Release Date	18th May 2018
Revision	73953
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

None

Improvements

1. 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 Issues

1. Current Time values on the [Dashboard] are not displayed correctly in Internet Explorer web browser
2. If Hardware Acceleration is enabled then Dial-In Users are unable to route to the Internet via the VPN tunnel using 'Use default gateway on remote network'

Firmware Version	3.8.8 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	14th February 2018
Release Date	14th March 2018
Revision	72017
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

New Features

1. LAN ports, Wireless LAN button and Factory Reset button can now be enabled or disabled from [System Maintenance] > [Panel Control]

2. Router's status LEDs & port LEDs can be turned off or put into "LED Sleep Mode" when inactive, configured in [System Maintenance] > [Panel Control]

3. Wireless Pre-Shared Key can now be viewed when logged into the router's admin account. Click on the "****" text to reveal the password currently in use

4. EAPOL Key Retry Enable/Disable setting added to [Wireless LAN (2.4GHz/5GHz)] > [Security] Disabling this setting can prevent WPA2 Key Reinstallation Attack (KRACK) attack vectors, for more details please read this security advisory:
   https://www.draytek.co.uk/information/our-technology/wpa2-krack-vulnerability
   (EAPOL Key Retry is set to Enabled by default and in previous firmware)

5. Anti-Spoofing Defence settings for IP and ARP spoofing added to [Firewall] > [Defence Setup]

6. ISO 3166 Country objects added to [Objects Setting] menu for use with Firewall Filter rules and Route Policy rules

7. Dashboard layout can be configured with the Customise Dashboard link at the bottom of the [Dashboard] page

Improvements

1. Speed and duplex settings manually configured for WAN1 / WAN2 ports could display incorrect status information

2. TR-069 parameters added for Bind IP to MAC configuration and comments

3. Disabling Bind IP to MAC with a specific configuration could block access to the router

4. DoS Defence moved to [Firewall] > [Defence Setup]

5. "None" option for Syslog in CSM (UCF/WCF/DNSF) profile is no longer used

6. Default WAN Connection Detection mode for PPPoE connections is now named "PPP Detect" instead of "ARP Detect"

7. Syslog & SMTP Server fields in [System Maintenance] > [Syslog/Mail Alert Setup] now allow up to 63 characters for longer hostnames

8. Web Syslog in [Diagnostics] > [Syslog Explorer] can now be used when "Syslog Server" is not enabled or configured in [System Maintenance] > [Syslog / Mail Alert]

9. User Management could not authenticate users with RADIUS when the RADIUS server was accessed through a VPN tunnel

10. The "IP Routed Subnet" option could not be enabled in [Bandwidth Management] > [Bandwidth Limit]

11. Bandwidth Limit's effect on LAN to LAN VPN tunnels is toggled on/off with the "IP Routed Subnet" option

12. Bandwidth Limit was not applied to VPN traffic correctly in some configurations
13. MyVigor DrayDDNS service status could incorrectly be displayed in red after updating information
14. [NAT] > [Open Port] settings could not be saved if a UDP port was specified that conflicted with a TCP management port
15. Failback setting option in [Routing] > [Load Balance/Route Policy] rules could not be saved in some configurations
16. Remote Dial-In Users connecting via PPTP protocol were not assigned DNS addresses configured for the LAN subnet
17. Improved DNS caching behaviour with Web Content Filtering and DNS Filtering enabled
18. Firmware could only be upgraded through Firmware Upgrade Utility 3.6.6 when router was manually put into TFTP mode

Known Issues

1. Current Time values on the [Dashboard] are not displayed correctly in Internet Explorer web browser
2. If Hardware Acceleration is enabled then Dial-In Users are unable to route to the Internet via the VPN tunnel using 'Use default gateway on remote network'

Firmware Version	3.8.7 (Formal Release)
Release Type	**Initial Release**
Build Date	27th October 2017
Release Date	15th January 2018
Revision	69532
Applicable Models	Vigor2926, Vigor2926n, Vigor2926ac
Locale	UK & Ireland Only

First Firmware Release for this model

New Features

(None)

Improvements

(None)

[END OF FILE]