Release Notes for WRVS4400N Version 2.0 Firmware 2.0.2.1

June 2011

These Release Notes describe updates and known issues in WRVS4400N firmware version 2.0.2.1.

⚠ CAUTION Firmware images that support the WRVS4400N v2.0 hardware are not backward-compatible with the WRVS4400N v1.0 and v1.1 hardware. Do *not* try to upgrade your v1.0 or v1.1 hardware with firmware that is intended for use with the v2.0. The same applies to the v1.0 and v1.1 hardware firmware versions. Older firmware versions cannot be loaded onto WRVS4400N v2.0 hardware.

Contents

This document includes the following topics:

Changes Since WRVS4400N Firmware Version 2.0.1.3

Updates

The following updates were made in firmware version 2.0.2.1:

- Updated the text of the Note field on the Wireless > WDS window.
- Added a logout link to the Home page.
- Updated the Firewall > Internet Access Policy window so that when a user adds an allow-rule policy, the user can only add allow rules to the policy, but not deny rules.
- Updated the Internet access policy so that it supports overnight scheduling.

Fixed Problems

The following problems were fixed in firmware version 2.0.2.1:

- The DHCPv6 section of the Setup > LAN section does not reflect the correct DHCPv6 starting and ending IP pool addresses.
- If the PPPoE username or password include special characters, the PPPoE connection fails.
- The Firewall > Internet Access Policy window displays the wrong message when you change **Deny** to **Allow**.
- Internet filtering does not work if GET and HOST are split.
- Messages prompting the user for acknowledgement display a **YES** button instead of an **OK** button.
- No example of a forbidden domain construct in the GUI.
- The Approved URLs list displays an incorrect example of the syntax of a URL.
- Typo in the error message that is displayed when entering an IP addresses that is already in the Approved Clients list.
- No validation for the IP address ranges in the Approved Clients list.
- There is an issue in the process of generating random certificates.

- In the L2 Switch > VLAN window, highlighting all VLANs (2–4) and deleting VLAN ranges is misleading because some of the selected items remain in the list.
- Rebooting the router causes clients on non-default VLANs to lose their IP addresses and acquire IP addresses from the default VLAN (1).
- The broadcast IP address should not be allowed as the Gateway address when adding route.
- Incorrect error message displayed when adding a duplicate static route.
- Daylight savings time is incorrect for Time Zone GMT -6 (Central Time US and Canada).
- User cannot use the WAN IP address to locally access the GUI using HTTPS.
- SMTP update is needed so that the user can enter the port number.
- HTML tags are displayed when the Disconnect button is clicked on the Summary window.
- Fixed several web interface vulnerabilities that could be exploited by a remote, unauthenticated user. For more information, see the following Cisco Security Advisory:

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f190.shtml

Changes Since WRVS4400N Firmware Version 2.0.0.8

Fixed Problems

The following problems were fixed in firmware version 2.0.1.3:

- Fixed an issue that caused the RIP packet size to grow larger over time.
- Fixed an issue that caused a duplicate “default route” entry to show up in the routing table.
- Fixed a session logout issue by enabling a Log Out button.
- Fixed an issue that caused the router to become unresponsive and unrecoverable after the reset button during a firmware upgrade.
- Fixed an issue in the SIP-ALG code that caused a blind call transfer from one IP Phone to another IP Phone to fail.
- Fixed both of the QuickVPN user name and password fields to support a character length of up to 32 characters maximum.
- Fixed an issue that caused some printers to be unable to print over an IPSec VPN tunnel between two physical locations.
- Fixed an issue that caused the TrendMicro ProtectLink Gateway feature to fail to filter URLs if a customer accessed the URL through search results when the approved URL list had any URL entered.
- Fixed an issue that caused IPv6 packets between different VLAN’s to not be blocked if inter-VLAN routing is disabled.
- Fixed an issue that caused a QuickVPN tunnel to not be re-established when more than “any” remote gateway is configured for the tunnel settings.
- Fixed an issue that caused port forwarding rules to stop if IPS was disabled.
- Fixed an issue that caused the DDNS status to always show “Please Wait” in the web-based management interface of the router.
- Fixed an issue that caused WDS to not allow more than one access point to connect to the WRVS4400N for wireless repeater support.
- Converted the style of the ProtectLink Gateway administration page to the style of the current ProtectLink Web administration page.
- Fixed an issue found in the Time Zone setting that caused the system time to be incorrect when the Time Zone is set to “(GMT-03:30) Newfoundland.”

- Fixed an issue in the SIP-ALG code that caused certain SIP packets to be tagged with the incorrect VLAN ID.
- Fixed an issue with WDS that caused the router wireless driver to be unresponsive when trying to get a WAP4410N access point to associate to WRVS4400N.
- Fixed an issue in the VPN code that caused the QuickVPN client to drop the connection when the QuickVPN client connects to the QuickVPN server behind a NAT router.

Known Issues

The following is a list of known issues:

- After the you log into the router's web-based configuration utility, you could open a new browser window or tab and access the configuration utility without having to re-authenticate.
- If your computer is on the same LAN as the WRVS4400N router, you cannot log into the router's web-based configuration utility using the router's WAN IP address. You must use the LAN IP address instead.
- The RIP network mask shows incorrectly when the VLAN LAN IP is set as 10.0.2.1.
- eMule(0.48a) can't be blocked by IPS.

Changes Since WRVS4400N Firmware Version 2.0.0.7

Updated the wireless driver to improve WLAN adapter interoperability between different WLAN adapter vendors.

Changes Since WRVS4400N Firmware Version 1.00.09

Problems were fixed.

Fixed Problems

The following problems were fixed in firmware version 2.0.2.1:

- Fixed an issue that caused voice packets to become incorrectly routed during call transfers between 3 or more IP phones.
- Fixed an issue that caused the QuickVPN client to not allow the complete transfer of more than 100 MB of a large file over a VPN tunnel.
- Fixed an issue in the SIP ALG where the session originator sends a packet with source port 1028, but the via port in the SIP message is 5060.
- Fixed an issue caused when the router does not map a 4-digit number to the correct IP address of a phone registered to at the SIP server.
- Corrected the pop-up message on the DMZ page to be “DMZ IP Address contains an invalid number.”
- Corrected the pop-up message on the DMZ page to be “DMZ IP Address is invalid. Valid range is 1 to 254.”
- Fixed an issue that caused the checking mechanism used on the Approved Clients IP page to function incorrectly.
- Corrected the text “Sec.” to be “sec” for the Key Lifetime filed on the IPSec VPN Tunnel setup page.
- Corrected the text for IP Conntrack window title to be “IP Conntrack” and not “IP Conntracks”.
- Corrected a spacing issue on the QoS Bandwidth Management page of the web-based GUI.
- Fixed an issue caused when using Firefox 3.5 to view the web-based GUI that caused the text on the navigation toolbar to become blurry.
- Fixed an issue with WLAN client performance in mixed mode environments that allows for increased interoperability with more WLAN clients.
- Corrected the text on the Firewall Port Range Forwarding page.

- Fixed an issue caused when the LAN IP address of the local router is used in the IPSec VPN Tunnel configuration for the remote group setting.
- Fixed an issue caused when the Timezone setting is changed, which caused ProtectLink URL filtering to become unstable.
- Fixed the Trend Micro Protectlink URL used during account registration. This URL is used by Trend Micro to identify which product is being used.
- Fixed an issue in the Firewall page that caused the page to be displayed incorrectly when clicking the Save button twice when accessing the router remotely via HTTPS.
- Fixed an issue that did not allow a fully-qualified domain name to be used in the Syslog server field.
- Changed the "O" field value of certificates from "Cisco" to "Cisco System, Inc."
- Fixed an issue that slowed Internet access after a user enabled the Trend Micro ProtectLink feature.
- Fixed and issue that caused outbound logging to become unstable.
- Fixed an issue that caused the router WAN setup page to display incorrectly when using Internet Explorer 7.
- Fixed an issue on the VPN setup page that caused the page to become unresponsive when adding a new IPSec policy.
- Fixed an issue that allowed the router to save invalid LAN IP.
- Fixed an issue on the Administration Management page that allowed duplicate usernames to be saved.
- Fixed an issue that caused the router VLAN IP to not save correctly.
- Fixed an issue on the IP Based ACL page that caused the check boxes to not become greyed out after clicking the "Disable All Rules" button.
- Fixed an issue on the VPN Summary page that shows the number of available IPSec VPN tunnels incorrectly.
- Fixed an issue that caused the router web-based GUI to not allow the removal of router usernames.
- Corrected a typo in the pop-up message that appeared when adding the same username to the Router Access page.

- Fixed an issue in the Traceroute feature to check for valid input before executing.
- Fixed an issue that allowed a user to configure and save an invalid character string in the Syslog Server field.
- Rebranded the web-based GUI from the Linksys to the Cisco design.
- Fixed an issue in the IPv6 DHCP server that caused the DHCP server to become unresponsive.
- Fixed the QVPN client so that it does not reconnect to the router after disconnecting.
- Fixed the QVPN connection to WRVS4400Nv1.1 so that the connection does not stay active.
- Improved DMZ WAN-to-LAN performance.
- Fixed Forbidden Domain failure. If *any* IP based ACL rules are present then the any Forbidden Domains or Keywords present in the Internet Access Policy are not be applied.
- Fixed an issue with DNS source port changing incorrectly.
- Fixed an issue that caused the PPTP passthrough to fail to connect to a PPTP server.
- Replaced the wireless default SSID with ciscosb.
- Fixed an issue that caused WDS not to be supported when the security mode is WPA/WPA2.
- Corrected the SNMP OID to 1.3.6.1.4.1.9.6.1.22.250.2.
- Updated the IPS code to not check for the old Linksys MAC address used before rebranding.

Known Issues

- RIP network mask shows incorrectly when setting a VLAN LAN IP as 10.0.2.1.
- eMule(0.48a) can’t be blocked by IPS.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
Cisco Wireless-N Gigabit Security Router with VPN WRVS4400N	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

OL-20703-01