Release Notes for Cisco RV220W Firmware Version 1.0.7.2

October 2015

These Release Notes describe the changes and known issues in Cisco RV220W firmware version 1.0.7.2.

IMPORTANT:

As with any firmware release, please read these release notes before upgrading the firmware. Cisco also recommends backing up your configuration before any firmware upgrade.

NOTE If you install firmware version 1.0.5.x and later need to revert to a previous firmware version (for example, 1.0.4.x), you must perform a factory reset during the downgrade. If you do not perform a factory reset when downgrading, future upgrades to firmware versions 1.0.5.x will fail.

Contents

This document includes the following topics:

- Issues Resolved in Version 1.0.7.2
- Known Issues
- Related Information

Issues Resolved in Version 1.0.7.2

- Management Authentication Bypass Vulnerability (CSCuv29574)
Release Notes

Known Issues

The following issues are known to occur in this version of the firmware. Read this information before upgrading.

Issues Carried Over from Release 1.0.6.6

- The 6to4 tunnel can not recover immediately after reloading the device. (CSCup65680)
  Workaround: Wait for 10 minutes.

Issues Carried Over from Release 1.0.5.8

- 802.1X does not work on the device. (CSCuj86918)
  Workaround: None.

- The total WAN (Internet) bandwidth limiting does not work correctly. (CSCul07244)
  Workaround: Use QoS profile rules to limit the stream bandwidth.

- When users change the IPv6 WAN to DHCP mode from static address mode, the WAN status down. (CSCul88869)
  Workaround: Reboot the device after you change the configuration.

- The Device is unable to send out email logs if it is configured to use a non-default logging policy. (CSCuj85135)
  Workaround: Use the default logging policy.

- A client cannot connect via SSL VPN with a corporate proxy setting. (CSCto14499)
  Work Around: Disable the proxy setting or set the proxy by using the IP address instead of the domain name. For example, in Internet Explorer, adjust the proxy settings by going to Tools > Internet Options. Click the Connections tab, and then click the LAN settings button. Proceed as needed:

  - To disable the proxy, uncheck the Use a proxy server box and then check the Automatically detect settings box. Click OK to save the changes, and then click OK to close the Internet Options window.

  OR
- **To identify the proxy by IP address:** Check the **Use a proxy server** box, delete the domain name if in use, and enter the IP address of the proxy server in the **Address** box.

- VPN connectivity can be lost when using SSL VPN port forwarding and later versions of Firefox. (CSTj59663)
  **Work Around:** Use Internet Explorer or Firefox version 3.6.17.

- When a Gateway To Gateway tunnel is configured in aggressive mode, the router cannot establish a connection to a Cisco RVS4000 or Cisco WRVS4400N router with a dynamic WAN IP address. (CSTt61631)
  **Work Around:** Configure a Gateway To Gateway tunnel in Main mode instead. On the **VPN > IPsec > Advanced VPN Setup** page, select the tunnel and then click **Edit**. Change the Exchange Mode to Main. When the VPN tunnel is configured in Main mode, the router can establish a connection. However, be aware that you will need to update the tunnel configuration whenever there is a change in the RVS4000’s dynamic IP address.

- A 6to4 tunnel may encounter packet loss depending on the type of NIC used. (CSTr08162)

- WAN QoS profile binding based on a particular services, such as FTP, may not work properly. (CSTu07893)
  **Work Around:** Select ANY as the service type when creating QoS profiles. This work around limits QoS bindings to the traffic selector match type (IP address Range, MAC address, VLAN, DSCP, and SSID) rather than service type. Due to this limitation you cannot overlap a particular traffic selector match type among the different QoS bindings.
## Related Information

<table>
<thead>
<tr>
<th>Support</th>
<th><a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Support Community</td>
<td></td>
</tr>
<tr>
<td>Cisco Support and Resources</td>
<td><a href="http://www.cisco.com/go/smallbizhelp">www.cisco.com/go/smallbizhelp</a></td>
</tr>
<tr>
<td>Phone Support Contacts</td>
<td><a href="http://www.cisco.com/go/sbsc">www.cisco.com/go/sbsc</a></td>
</tr>
<tr>
<td>Cisco Firmware Downloads</td>
<td><a href="http://www.cisco.com/go/smallbizfirmware">www.cisco.com/go/smallbizfirmware</a></td>
</tr>
<tr>
<td></td>
<td>Select a link to download firmware for Cisco Products. No login is required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco RV220W</td>
<td></td>
</tr>
<tr>
<td>Cisco Partner Central (Partner Login Required)</td>
<td><a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a></td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.