Release Notes for Cisco RV160x and RV260x Router Firmware Version up to 1.0.01.01

September 2020

This document describes resolved issues and known issues in Cisco RV160x and RV260x Firmware Version 1.0.01.01.

NOTE From this release, Web filtering feature 1-year subscription is enforced. Please upgrade your device in order to renew the subscription.

Improvements

- Update ASDv2 to ASDv3
- Web filtering license renew enhancement
- Network booting option to support PXE bootup - Network booting or netboot is the process of booting a computer from a network rather than a local drive.
- Optimize wireless stability
- Other GUI minor fixes

Contents

Resolved Issues

Resolved Issues from Release 1.0.01.01

Number	Description
CSCvr08796	Evaluation of pp for Kr00k attack - CVE-2019-15126
CSCvr08789	Error creating Site-to-Site VPN when remote network is supernet of local network.
CSCvr07923	Timezone incorrect when DST is enabled.
CSCvt39790	Evaluation of pp for pppd buffer overflow vulnerability.
CSCvt39791	Evaluation of pp for pppd buffer overflow vulnerability.
CSCvv34032	On WAN interface is not possible to configure a /31 subnet mask.
CSCvr08796	RV160x/260x: Traffic to router doesn't work if Site-to-Site VPN uses supernet of local network
CSCvv34032	RV260W: On WAN interface is not possible to configure a /31 subnet mask

Resolved Issues from Release 1.0.00.17

Number	Description
CSCvt23810	Evaluation of pp for Kr00k attack - CVE-2019-15126

Resolved Issues from Release 1.0.00.16

Number	Description
CSCvn50444	Errors with some countries in list for CSR.
CSCvn99887	WAN port goes down when configured "100 Full”.
CSCvn96172	Can't connect to PPTP Server behind router.
CSCvp84524	Cisco Small Business RV160 / 260 Static credentials vulnerability.

Number	Description
CSCvp84558	Cisco RV160 / 260 Hardcoded password hashes
CSCvp84480	Cisco RV160 / 260 Unwanted software embedded: GNU Debugger (gdb).
CSCvp84505	Cisco RV160 / 260 Unwanted software embedded: tcp dump.
CSCvq54631	[CFD] CSCvp73955 Evaluate Cisco RV34x for CVE-2015-7547 vulnerability.
CSCvq52858	Evaluation of pp for TCP MSS/SACK DoS vulnerabilities. (RV160x)
CSCvq52859	Evaluation of pp for TCP MSS/SACK DoS vulnerabilities. (RV260x)

Resolved Issues from Release 1.0.00.15

Number	Description
CSCvn27058	GUI displayed abnormal when the browser/OS is set to German, French, Italian, Spanish.
CSCvn27041	The device is booted with old version after upgrading by PnP.

Known Issues

Known Issues from Release 1.0.00.15

Number	Description
CSCvg83154	Intermittent packet loss observed when WAN interface is linked as 10M bps. **Solution:** None.

Number	Description
CSCvh03499	Cisco IP phone C9XX connection to disabled PoE port will cause the DUT LAN port not to work. **Solution:** Connect the phone to the RV260P PoE port and power the router. Or configure the RV260P LAN port as 100M full instead of Auto Negotiation.
CSCvh49249	IKEv2 S2S tunnel will not work with ASA. **Solution:** Use IKEv1 instead.
CSCvi25236	LAN 100M mode IoT issue with WAP581. **Solution:** Set both RV router and WAP581 as auto-negotiation mode. Or place a switch in between.
CSCvj08450	IKEv2 multiple subnets working with ISR/ASR routers is not supported. **Solution:** Use IKEv1 if multiple subnet support is needed.
CSCvj10961	GRE interface name containing " _" characters will cause the tunnel to not function. **Solution:** Remove the " _" from the GRE name.
CSCvj43875	Captive Portal logo cannot show correctly when a file name includes a special character. **Solution:** Do not include a space character in the file name.
CSCvj53075	Policy NAT will not work well when the IP address group include multiple entries. **Solution:** Only the last one will work if the address group contains multiple entries.
CSCvj66506	Static dhcp entries shown as dynamic in the dhcp binding table. **Solution:** None.

Number	Description
CSCvj76246	System time will sync with ntp server when configured manually if PnP is enabled. **Solution:** Disable the PnP feature if the manual time setting is required.

Known Issue from Release 1.0.00.13

Number	Description
CSCvg83154	Intermittent packet loss observed when WAN interface is linked as 10M bps. **Solution:** None.
CSCvh03499	Cisco IP phone C9XX connection to disabled PoE port will cause the DUT LAN port not to work. **Solution:** Connect the phone to the RV260P PoE port and power the router. Or configure the RV260P LAN port as 100M full instead of Auto Negotiation.
CSCvh49249	IKEv2 S2S tunnel will not work with ASA. **Solution:** Use IKEv1 instead.
CSCvi25236	LAN 100M mode IoT issue with WAP581. **Solution:** Set both RV router and WAP581 as auto-negotiation mode. Or place a switch in between.
CSCvj08450	IKEv2 multiple subnets working with ISR/ASR routers is not supported. **Solution:** Use IKEv1 if multiple subnet support is needed.
CSCvj10961	GRE interface name containing " _" characters will cause the tunnel to not function. **Solution:** Remove the " _" from the GRE name.

Number	Description
CSCvj43875	Captive Portal logo cannot show correctly when a file name includes a special character. **Solution:** Do not include a space character in the file name.
CSCvj53075	Policy NAT will not work well when the IP address group include multiple entries. **Solution:** Only the last one will work if the address group contains multiple entries.
CSCvj66506	Static dhcp entries shown as dynamic in the dhcp binding table. **Solution:** None.
CSCvj76246	System time will sync with ntp server when configured manually if PnP is enabled. **Solution:** Disable the PnP feature if the manual time setting is required.

Firmware Auto Fallback Mechanism

The device includes two firmware images in the flash to provide an Auto Fallback Mechanism so that the device can automatically switch to the secondary firmware when the active firmware is corrupted or cannot boot up successfully.

The Auto Fallback Mechanism operates as follows:

STEP 1 The device first boots up with the active firmware.

STEP 2 If the active firmware is corrupted, it will switch to the secondary firmware automatically, after the active firmware has failed to boot up after 5 trials. If the router gets stuck and does not reboot automatically to the secondary image, proceed to do the following:

- Power the router off.
- Power the router back on, and wait for 30 seconds, then power off.

- Repeat Step 2 for 5 times. The router will switch to the secondary or inactive firmware.

STEP 3 Re-download the firmware and check the flash or reset to factory default settings to see if any configuration settings are causing the issue.

Related Information

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Cisco Firmware Downloads	www.cisco.com/go/software Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco RV Series Routers	www.cisco.com/go/smallbizrouters

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. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.