

# Release Notes for Cisco RV 160x and RV260x Router Firmware Version up to 1.0.01.04

## August 2021

This document describes resolved issues and known issues in Cisco RV 160x and RV260x Firmware Version 1.0.01.04. The configuration will be lost if you downgrade the firmware from this version to an earlier version. The configuration files from this version can not be imported to the previous release. We highly recommend to backup the router configuration before upgrading the firmware.

The most common configurations on the older releases are supported on the new version and can be kept after upgrading. However, we recommend that you reset your device to use the default settings when you upgrade to this version and reconfigure your device as there are many new features and changes on this version.

## Note

- Cisco will no longer support new USB modems/dongles for RV260/260P/260W models, effective January 2021.
- Web filtering feature 1-year subscription is enforced in all prior 1.0.01.02 RV260 series releases. Please upgrade your device in order to renew the subscription.

## New Features and Improvements

- Support Layer2 port level statistics in SNMP ifTable/ifXTable.

### Contents

- **Resolved Issues from Release 1.0.01.04**
- **Known Issues**
- **Firmware Auto Fallback Mechanism**
- **Related Information**

### Resolved Issues from Release 1.0.01.04

Number	Description
<b>CSCvw95016</b>	Cisco Small Business RV Series Routers Link Layer Discovery Protocol vulnerabilities
<b>CSCvy02177</b>	New CDP memory leak vulnerability.
<b>CSCvy02232</b>	Cisco Small Business RV 160 and RV260 Series Routers Remote Command Execution Vulnerability.

### Resolved Issues from Release 1.0.01.03

Number	Description
<b>CSCvx24759</b>	RV 160x/260x: IPsec tunnels don't work after upgrading to 1.0.01.02
<b>CSCvw99580</b>	RV 160x/260x: Radius server retry count does not work as expected.
<b>CSCvw83406</b>	RV260x: Open VPN client fails to connect and gives "fragment directive" error message.
<b>CSCvw83787</b>	Multiple vulnerabilities in dnsmasq DNS Forwarder affecting Cisco Products: January 2021 (RV 160x).
<b>CSCvw83788</b>	Multiple vulnerabilities in dnsmasq DNS Forwarder affecting Cisco Products: January 2021 (RV260x).
<b>CSCvw62413</b>	RV 160x/260x: Ildp Stack overflow vulnerability.
<b>CSCvw62417</b>	RV 160x/260x: Ildp Assertion failure vulnerability.

Number	Description
<b>CSCvw92723</b>	RV160x/260x: Upload authorization bypass vulnerability.

## Resolved Issues from Release 1.0.01.02

Number	Description
<b>CSCvu36716</b>	RV260: LAG failover sometimes not happening.
<b>CSCvv59839</b>	RV160x/260x: CSR certificate details not displayed in GUI.
<b>CSCvv79432</b>	VLAN8 interface shown as “VDMZ” in the dropdown list when editing Access Rule.
<b>CSCvo60234</b>	TX counter is 0, and two tunnels are created when Shrewcroft dials in from Linux.
<b>CSCvr26013</b>	RV160/RV260: Dynamic DNS username does not accept “:”, “%”, or “#” characters.
<b>CSCvw13908</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
<b>CSCvw13917</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
<b>CSCvw19718</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
<b>CSCvw19849</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
<b>CSCvw19856</b>	Cisco SBRV160, RV160W, RV260, RV260P and RV260W Arbitrary File Write Vulnerabilities.
<b>CSCvw19878</b>	Cisco SB RV160 and RV260 Series Non-exploitable Unauthenticated Directory Traversal Issue.
<b>CSCvw22856</b>	Cisco SB RV160, RV160W, RV260, RV260P & RV260W Arbitrary File Write Vulnerabilities.
<b>CSCvw27923</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.

## Release Notes

---

Number	Description
<b>CSCvw27982</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
<b>CSCvw50568</b>	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.

### Resolved Issues from Release 1.0.01.01

Number	Description
<b>CSCvr08796</b>	Evaluation of pp for Kr00k attack - CVE-2019-15126.
<b>CSCvr08789</b>	Error creating Site-to-Site VPN when remote network is a supernet of local network.
<b>CSCvr07923</b>	Timezone incorrect when DST is enabled.
<b>CSCvt39790</b>	Evaluation of pp for pppd buffer overflow vulnerability.
<b>CSCvt39791</b>	Evaluation of pp for pppd buffer overflow vulnerability.
<b>CSCvv34032</b>	On WAN interface is not possible to configure a /31 subnet mask.
<b>CSCvr08796</b>	RV 160x/260x: Traffic to router doesn't work if Site-to-Site VPN uses supernet of local network.
<b>CSCvv34032</b>	RV260W: On WAN interface it is not possible to configure a /31 subnet mask.

### Resolved Issues from Release 1.0.00.17

Number	Description
<b>CSCvt23810</b>	Evaluation of pp for Kr00k attack - CVE-2019-15126.

## Resolved Issues from Release 1.0.00.16

Number	Description
<b>CSCvn50444</b>	Errors with some countries in list for CSR.
<b>CSCvn99887</b>	WAN port goes down when configured "100 Full".
<b>CSCvn96172</b>	Can't connect to PPTP Server behind router.
<b>CSCvp84524</b>	Cisco Small Business RV160 / 260 Static credentials vulnerability.
<b>CSCvp84558</b>	Cisco RV 160/260 Hardcoded password hashes.
<b>CSCvp84480</b>	Cisco RV 160 / 260 Unwanted software embedded: GNU Debugger (gdb).
<b>CSCvp84505</b>	Cisco RV 160/260 Unwanted software embedded: tcp dump.
<b>CSCvq54631</b>	[CFD] CSCvp73955 Evaluate Cisco RV34x for CVE-2015-7547 vulnerability.
<b>CSCvq52858</b>	Evaluation of pp for TCP MSS/SACK DoS vulnerabilities. (RV160x)
<b>CSCvq52859</b>	Evaluation of pp for TCP MSS/SACK DoS vulnerabilities. (RV260x)

## Resolved Issues from Release 1.0.00.15

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

## Known Issues

### Known Issues from Release 1.0.01.02

Number	Description
<b>CSCvw99580</b>	RADIUS retry count does not work. <b>Solution:</b> Always send two retry packets.

### Known Issues from Release 1.0.00.15

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

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

### Known Issue from Release 1.0.00.13

Number	Description
<b>CSCvg83154</b>	<p>Intermittent packet loss observed when WAN interface is linked as 10M bps.</p> <p><b>Solution:</b> None.</p>
<b>CSCvh03499</b>	<p>Cisco IP phone C9XX connection to disabled PoE port will cause the DUT LAN port not to work.</p> <p><b>Solution:</b> 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.</p>
<b>CSCvh49249</b>	<p>IKEv2 S2S tunnel will not work with ASA.</p> <p><b>Solution:</b> Use IKEv1 instead.</p>

## Release Notes

---

Number	Description
<b>CSCvi25236</b>	LAN 100M mode IoT issue with WAP581. <b>Solution:</b> Set both RV router and WAP581 as auto-negotiation mode. Or place a switch in between.
<b>CSCvj08450</b>	IKEv2 multiple subnets working with ISR/ASR routers is not supported. <b>Solution:</b> Use IKEv 1 if multiple subnet support is needed.
<b>CSCvj10961</b>	GRE interface name containing “_” characters will cause the tunnel to not function. <b>Solution:</b> Remove the “_” from the GRE name.
<b>CSCvj43875</b>	Captive Portal logo cannot show correctly when a file name includes a special character. <b>Solution:</b> Do not include a space character in the file name.
<b>CSCvj53075</b>	Policy NAT will not work well when the IP address group includes multiple entries. <b>Solution:</b> Only the last one will work if the address group contains multiple entries.
<b>CSCvj66506</b>	Static dhcp entries shown as dynamic in the dhcp binding table. <b>Solution:</b> None.
<b>CSCvj76246</b>	System time will sync with ntp server when configured manually if PnP is enabled. <b>Solution:</b> 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 five trials. If the router gets stuck and does not reboot automatically to the secondary image, do the following:
    - Power the router off.
    - Power the router back on and wait for 30 seconds, then power it off.
    - Repeat Step 2 for five 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

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

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](http://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)

© 2021 Cisco Systems, Inc. All rights reserved.