Release Notes for Cisco RV160x and RV260x Router Firmware Version up to1.0.01.08

Contents

Cisco RV160x and 260x Router Firmware Version 1.0.01.08

May 2022

This document describes resolved issues and known issues in Cisco RV160x and RV260x Firmware Version 1.0.01.08. 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.

IMPORTANT NOTE

A new firmware installation verification mechanism is optimized to reject invalid images. DO NOT downgrade the Firmware from 1.0.01.08 to 1.0.01.05 or other earlier versions.
If you really want to downgrade, select inactive version (1.0.01.05 or earlier) then reboot the router. If you have downgrade issues, please call Cisco support.
Some of the configuration options may not be compatible when the firmware is downgraded.
If some of the features do not work after the firmware downgrade please reset the device to factory default settings and reconfigure the device or restore a copy of the previously backed up configuration file with the downgraded or earlier firmware version.

We highly recommend you to backup your configurations first before upgrading or downgrading your device.

New Features and Improvements

- Added DHCP NAK option to bypass the Server-ID check for specific scenarios.
- Enhanced debug collection for wireless 5G radios.

Resolved Issues from Release 1.0.01.08

The following table lists the resolved issues in firmware 1.0.01.08

Number	Description
CSCwa72215	Failed to provision configuration file on rv26x by PnP.
CSCwa92233	Router DHCP custom option to bypass NAK processing for the specific scenario.

Number	Description
CSCvy93281	SNMP LAN port stats retrieval optimizations.
CSCwa71839	IKEv2 S2S issues Keep-alive issue: S2S tunnel only attempts to negotiate once. IKEv2 S2S issues: PSK with backslash.
CSCwa95371	SNMP security-level buffer overflow when injecting a long string.

Cisco RV160x and 260x Router Firmware Version 1.0.01.07

January 2022

This document describes resolved issues and known issues in Cisco RV160x and RV260x Firmware Version 1.0.01.07. 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.

We highly recommend you to backup your configurations first before upgrading or downgrading your device.

Note

- Effective January 2021, Cisco is not adding support for new USB modems/ dongles on RV260/260P/260W.
- Web filtering feature on RV260: 1 Year subscription is enforced in all firmware releases prior to 1.0.01.02. Please upgrade your device to renew the subscription.

New Features and Improvements

- Supports IKEv2 Non-RFC option to work with various VPN peers with multiple subnet.
- Supports DH Group14 2048bit for IKEv2 profile.
- Optimized wireless stability and add more logs.

Resolved Issues from Release 1.0.01.07

The following table lists the resolved issues in firmware 1.0.01.07

Number	Description
CSCwa67247	PnP should use short PID without country suffix.
CSCwa72154	Certificate display issue with key length 3072bits.
CSCwa13115	Cisco Small Business RV Series Routers Digital Signature Verification Bypass vulnerability.
CSCwa13682	Cisco Small Business RV Series Routers SSL Certificate Validation vulnerability.
CSCwa14007	Cisco Small Business RV Series Routers Open Plug N Play Command Injection vulnerability.
CSCwa14564	Cisco Small Business Routers Privilege Escalation vulnerability.
CSCwa1567	Cisco Small Business Routers Privilege Escalation vulnerability.

Known Issues from Release 1.0.01.07

The following table lists the known issues in firmware 1.0.01.07

Number	Description
CSCwa72215	Failed provision configuration file on rv26x/rv16x by pnp.

Number	Description
CSCwa72142	Firmware downgrade issue when using external radius server. **Solution:** Export the configuration file, reset the device to factory default setting, then import the configuration back in.

Cisco RV160x and 260x Router Firmware Version 1.0.01.05

Resolved Issues from Release 1.0.01.05

The following table lists the resolved issues in firmware 1.0.01.05

Number	Description
CSCvz55531	Email fails with "the server sent an empty reply" entry in the log.
CSCvy93232	RV260: SNMP getBulkRequest against interface OIDs causes "genErr (5)" message.
CSCvy94326	RV260W DST (Daylight saving time) is not working after a reboot.
CSCvy97652	RV16/260: WAN PPPoE with VLAN tag is not getting the IP Address after reboot.
CSCvy93972	Email user name does not accept entries longer than 32 characters.

Cisco RV160x and 260x Router Firmware Version 1.0.01.04

Resolved Issues from Release 1.0.01.04

The following table lists the resolved issues in firmware 1.0.01.04

Number	Description
CSCvw95016	Cisco Small Business RV Series Routers Link Layer Discovery Protocol vulnerabilities
CSCvy02177	New CDP memory leak vulnerability.
CSCvy02232	Cisco Small Business RV160 and RV260 Series Routers Remote Command Execution Vulnerability.

Cisco RV160x and 260x Router Firmware Version 1.0.01.03

Resolved Issues from Release 1.0.01.03

The following table lists the resolved issues in firmware 1.0.01.03

Number	Description
CSCvx24759	RV160x/260x: IPSec tunnels don't work after upgrading to 1.0.01.02
CSCvw99580	RV160x/260x: Radius server retry count does not work as expected.
CSCvw83406	RV260x: Open VPN client fails to connect and gives "fragment directive" error message.
CSCvv83787	Multiple vulnerabilities in dnsmasq DNS Forwarder affecting Cisco Products: January 2021 (RV160x).
CSCvv83788	Multiple vulnerabilities in dnsmasq DNS Forwarder affecting Cisco Products: January 2021 (RV260x).
CSCvw62413	RV160x/260x: lldp Stack overflow vulnerability.
CSCvw62417	RV160x/260x: lldp Assertion failure vulnerability.

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

Cisco RV160x and 260x Router Firmware Version 1.0.01.02

Known Issues from Release 1.0.01.02

The following table lists the known issues in firmware 1.0.01.02

Number	Description
CSCvw99580	RADIUS retry count does not work. **Solution:** Always send two retry packets.

Resolved Issues from Release 1.0.01.02

The following table lists the resolved issues in firmware 1.0.01.02

Number	Description
CSCvu36716	RV260: LAG failover sometimes not happening.
CSCvv59839	RV160x/260x: CSR certificate details not displayed in GUI.
CSCvv79432	VLAN8 interface shown as “VDMZ” in the dropdown list when editing Access Rule.
CSCvo60234	TX counter is 0, and two tunnels are created when Shrewcroft dials in from Linux.
CSCvr26013	RV160/RV260: Dynamic DNS username does not accept “.”, “%”, or “#” characters.
CSCvw13908	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
CSCvw13917	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.

Number	Description
CSCvw19718	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
CSCvw19849	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
CSCvw19856	Cisco SBRV160, RV160W, RV260, RV260P and RV260W Arbitrary File Write Vulnerabilities.
CSCvw19878	Cisco SB RV160 and RV260 Series Non-exploitable Unauthenticated Directory Traversal Issue.
CSCvw22856	Cisco SB RV160, RV160W, RV260, RV260P & RV260W Arbitrary File Write Vulnerabilities.
CSCvw27923	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
CSCvw27982	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.
CSCvw50568	Cisco SB RV160, RV160W, RV260, RV260P, and RV260W VPN Routers RCE Vulnerabilities.

Cisco RV160x and 260x Router Firmware Version 1.0.01.01

Resolved Issues from Release 1.0.01.01

The following table lists the resolved issues in firmware 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 a 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.

Number	Description
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 it is not possible to configure a /31 subnet mask.

Cisco RV160x and 260x Router Firmware Version 1.0.00.17

Resolved Issues from Release 1.0.00.17

The following table lists the resolved issues in firmware 1.0.01.17

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

Cisco RV160x and 260x Router Firmware Version 1.0.00.16

Resolved Issues from Release 1.0.00.16

The following table lists the resolved issues in firmware 1.0.01.16

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.
CSCvp84558	Cisco RV160/260 Hardcoded password hashes.

Number	Description
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)

Cisco RV160x and 260x Router Firmware Version 1.0.00.15

Resolved Issues from Release 1.0.00.15

The following table lists the resolved issues in firmware 1.0.01.15

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 from Release 1.0.00.15

The following table lists the known issues in firmware 1.0.01.15

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

Number	Description
[illegible]	GRE interface name containing "_" character will cause the tunnel to not work. **Solution:** Remove the "_" from the GRE name.
[illegible]	Cisco IP phone 69XX connecting to disabled PoE port will cause the DUT LAN port. **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.
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.
CSCvh49249	IKEv2 S2S tunnel will not work with ASA. **Solution:** Use IKEv1 instead.
[illegible]	Policy NAT mode does not work when the IP address group include multiple entries. **Solution:** Only the first one will work if the address group contains multiple entries.
[illegible]	LAN 100M full duplex issue with WAP581. **Solution:** Set both RV router and WAP581 as auto-negotiation mode. Or replace 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.
CSCvj66506	Static dhcp entries are shown as dynamic in the dhcp binding table. **Solution:** None.

Number	Description
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 are shown as dynamic in the dhcp binding table. **Solution:** None.

Cisco RV160x and 260x Router Firmware Version 1.0.00.13

Known Issues from Release 1.0.00.13

The following table lists the known issues in firmware 1.0.01.13

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 includes 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.

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

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