Release Notes for Cisco RV134W up to Firmware Version 1.0.1.21

March 2021

This document describes known and resolved issues in the Cisco RV134W firmware version 1.0.1.21

Contents

Whats New

- Security Enhancement

Resolved Issues

Caveats Resolved in Release 1.0.1.21

Number	Description
CSCvw65032	Cisco Router RV134W stack-overflow vulnerability. **Solution:** Fixed
CSCvx45608	RV134W for CVE-2020-12695 UPnP CallStranger Vulnerability. **Solution:** Fixed
CSCvw62410	lldp stack-overflow vulnerability. **Solution:** Fixed
CSCvw62411	lldp Assertion Failure vulnerability. **Solution:** Fixed
CSCvw94341	lldpd used in router RV134 suffers from a memory leak vulnerability. **Solution:** Fixed
CSCvt39815	RV134W for pppd buffer overflow vulnerability. **Solution:** Fixed

Caveats Resolved in Release 1.0.1.20

Number	Description
CSCvs37094	Apply BRCM patch for Kr00k attack - CVE-2019-15126 **Solution:** Fixed

Caveats Resolved in Release 1.0.1.19

Number	Description
CSCvq31951	Evaluation of RV134W for TCP SACK vulnerabilities. **Solution:** Fixed

Caveats Resolved in Release 1.0.1.17

Number	Description
CSCvm22092	Failure when uploading the config file. **Solution:** Fixed
CSCvk00961	Radio turns off frequently after reboot. **Solution:** Fixed.

Caveats Resolved in Release 1.0.1.11

Number	Description
CSCvh60170	Remote Code Execution and Denial of Service Vulnerability. **Solution:** Fixed
CSCvh60172	Unauthenticated Information Disclosure Vulnerability. **Solution:** Fixed

Caveats Resolved in Release 1.0.0.29

Number	Description
CSCvb77787	Request to add ability to configure the WAN speed/ duplex. **Solution:** Fixed
CSCvb66642	Request for the ability to configure multiple addresses for a remote access. **Solution:** Fixed.
CSCvb66655	Not able to add a PTM entry for the xDSL WAN. **Solution:** Fixed
CSCvb66679	Not able choose a PTM entry for the xDSL WAN default route. **Solution:** Fixed
CSCva85081	Port Forwarding stops working after a while. **Solution:** Fixed
CSCvc84242	Inter-VLAN is not working correctly. **Solution:** Fixed

Dongle Support

The RV134W now supports the NETGEAR AirCard 320U dongle.

Firmware Recovery Steps

If the firmware corrupts during the upgrade or a power outage, the PWR LED light turns red. Please follow these steps to upload and recover the firmware.

STEP 1 Power off the router.

STEP 2 There are 2 ways to access the firmware recovery mode. You can select any of the following options to access the recovery mode.

- If the firmware is corrupt and the router is unable to boot normally, the router will automatically go into recovery mode after the device is powered on. The PWR LED will turn red. Usually, the original configuration will be restored after the new firmware is uploaded.
- To enter the recovery mode manually, connect the console cables (baud rate 115200) to the router. Power on the router and the boot up log will be displayed on the console terminal. Press any key to stop the normal startup. The PWR LED will turn red. Usually, the original configuration is restored after the new firmware is uploaded.
- To delete the original configurations on the router, press the reset button and power on the router.

STEP 3 Connect the PC to the LAN1 port. Configure the PC's static address as 192.168.1.100.

STEP 4 Recover the firmware to the router via web UI. For example, you can enter "http://192.168.1.1" in the browser, then choose the image like (for RV132W) "RV132W_FW_ANNEX_A_1.0.0.10.bin" and press Recover & Reboot. Wait for several minutes until the router reboots itself once the upload is completed and is flashing.

STEP 5 After the router starts up normally, the PWR LED will turn green.

Firmware Upgrade

To update the router with a newest version of the firmware, follow these steps from the router's graphical user interface (GUI).

STEP 1 Select **Administration > Firmware Upgrade**.

STEP 2 In the **Download the latest firmware** section, click **Download** to download the latest firmware version from Cisco.com.

STEP 3 In the **Locate & select the upgrade file** section, click **Browse** to locate and upload the firmware upgrade file.

STEP 4 Check **Reset all configuration/setting to factory defaults** to reset all the configurations and apply factory default settings.

STEP 5 Click **Start Upgrade** to update the firmware on the device. The device will automatically reboot after the update is completed.

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