Release Notes for Cisco RV320/RV325 Routers Firmware up to Version 1.5.1.11

June 2020

This document describes resolved issues and known issues in Cisco RV320/ RV325 Firmware Version 1.5.1.11.

NOTE **Since firmware version 1.5.1.11, the exported configuration file will be encrypted. Before upgrading, export the configuration file from old release, then upgrade to 1.5.1.11. Normally the configuration should be kept after upgrading. Just in case if any of the settings get lost, the 1.5.1.11 firmware will not accept the old configuration file. The User must downgrade to the original firmware version, load the configuration file, then upgrade again.**

What's New

- The USB device Update GUI page removed.
- Encrypt the exported configuration file.

Contents

Resolved Issues

Issues Resolved in Release 1.5.1.11

Number	Description
CSCvt26490	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability

Number	Description
CSCvt26504	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability
CSCvt26525	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26555	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability
CSCvt26591	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26619	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26643	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26659	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability.
CSCvt26663	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26669	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability.
CSCvt26676	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability.
CSCvt26683	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability.
CSCvt26705	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26714	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability.
CSCvt26718	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt26725	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.

Number	Description
CSCvt26729	Cisco Small Business RV320 and RV325 Routers Stack Overflow Vulnerability.
CSCvt39803	Evaluation of rv320 for pppd buffer overflow vulnerability.
CSCvt39804	Evaluation of rv325 for pppd buffer overflow vulnerability.

Issues Resolved in Release 1.5.1.05

Number	Description
CSCvq34465	Cisco RV320 Dual Gigabit WAN VPN Router static certificates and keys.
CSCvq34472	Cisco RV320 Dual Gigabit WAN VPN Router static password hashes.
CSCvq34469	Cisco RV320 Dual Gigabit WAN VPN Router static SSH key.
CSCvq34453	Evaluate Cisco RV320 Dual Gigabit WAN VPN Router for OpenSSL vulnerabilities.
CSCvq34450	Evaluate Cisco RV320 Dual Gigabit WAN VPN Router for Dnsmasq vulnerabilities.
CSCvq76761	RV32x: Information leakage in RV325 router.
CSCvq76768	RV320x: Command injection via the NTP server name.
CSCvq76776	RV320: Hidden commands in the CLI.
CSCvq34456	Evaluate Cisco RV320 Dual Gigabit WAN VPN Router for UPnP vulnerabilities.

Issues Resolved in Release 1.5.1.04

Number	Description
CSCvq00109	RV320 View System Log function does not work with the special configuration.
CSCvq00118	RV320 prints too many kern alert log messages when the UPnP is on.

Number	Description
CSCvq01764	RV320 - No DNS packets sent out from the WAN2 interface with an indirect primary WAN1 failover.
CSCvm78058	RV32x: Unauthenticated command injection vulnerability.
CSCvn70400	RV32x: S2S VPN traffic not restored after WAN IP is updated and the VPN is reconnected.
CSCvo03234	RV32x: doesn't drop TCP (SYN-FIN) packets.
CSCvm19335	JOR RV320 no Internet connectivity with Dongle E3372-153 Hi-Link mode.
CSCvg85922	RV32x Router's configuration file is accessed from the WAN/LAN without authentication.
CSCvb36323	RV32x: UPnP errors seen in logs.
CSCvf98348	RV32x: DSCP/ToS is reset to 0 for inbound traffic.
CSCvc70025	RV32x: Vulnerable version of samba in use.
CSCvg36824	RV32x: Disable weak SSL/TLS protocols and ciphers.
CSCvc97920	Password field with auto-complete enabled.
CSCvc97933	SSL cookie without secure flag set.
CSCvc97927	Strict transport security not enforced.
CSCvc97941	Cookie without HTTPOnly flag set.
CSCvc97944	Cacheable HTTPS response.
CSCvk51098	RV325 intermittent WAN failover recovery fails.
CSCvj94337	RV325: SIP packets are routed out to the WAN2 interface with a WAN1 source IP during indirect failover.
CSCvj37974	RV325 fails to assign static default gateway and DNS IP address of .255 for WAN.
CSCvg09486	RV32x: Can't create username longer than 11 characters.
CSCvh57077	RV32x: Not responding to Samsung phone DHCP Discover.
CSCvh65180	RV32x: Events are shown at the same time in logs.

Number	Description
CSCvf35230	RV32: Request for OpenVPN certificates to support SHA-1 and SHA-2.
CSCvc53242	RV32x: Disable default behavior of listening to UDP port 500.
CSCux66849	RV32x open resolver vulnerability.
CSCvc07956	Wrong group VPN connection list displayed.
CSCvc46518	RV32x: “Inbound Local Balance” domain name needs to support the minimum 131 character length FQDN requirement.
CSCuu99804	RV32x needs to support more than 15 characters in the DHCP Option 66.
CSCvb21382	RV32x: Can't send emails (logs) if the SMTP server password contains “%”
CSCve24459	RV32x: Clients not receiving IPv6 addresses if the VLAN1 is excluded.
CSCve34323	RV32x: OpenVPN users disappear if the user is deleted.
CSCvb85380	Fail to connect OpenVPN with the username 123qweASD!@#
CSCvf54339	RV32x: Web Filtering blocks the port forwarding for ports 80 and 443.
CSCva43065	RV32x: Access to the internal web server is broken when the web filtering is enabled.
CSCvb85995	RV320: Unchecked “Mirror all WAN and LAN traffic to Port 1" still mirrors port.
CSCvb88872	Old Syslog remains after device factory default reset.
CSCuw73597	RV32x: Online help update since Cisco VPN Client is no longer available.
CSCvc76104	RV325: 1:1 NAT hairpinning is broken.
CSCva91937	Router crashes due to large packet header. Crashes at skb_push() in packet_rcv() function.

Number	Description
CSCvc48735	RV32x: Only two IPSec VPN clients can connect.
CSCvc53327	No DHCP offer when the host name includes spaces.
CSCvg85922	RV32x Router's config file is accessed from the WAN/LAN without authentication.

Issues Resolved in Release 1.4.2.22

Number	Description
CSCvg85922	Cisco RV320 and RV325 routers information disclosure vulnerability.
CSCvm78058	Cisco RV320 and RV325 routers command injection vulnerability.
CSCvp09589	Cisco RV320 and RV325 routers Online Help reflected cross-site scripting vulnerability.
CSCvp09573	Cisco RV320 and RV325 routers weak credential encryption vulnerability.

Known Issues

Issues Carried over from Release 1.3.1.13

Number	Description
CSCuv45571	RV32x router One-to-One NAT fails to work properly after upgrading to v1.2.1.13. **Workaround:** User will require to reconfigure One-to-One NAT setting and specify the WAN interface again

Issues Carried over from Release 1.3.1.12

Number	Description
CSCux99100	RV320: DDNS account longer than 11/12 symbols is not accepted. **Workaround:** None

Issue Carried over from Release 1.1.1.19

Number	Description
CSCul83582	When using a VLAN that is subnetted with /25 subnet mask or higher, error appears when trying to configure Port Forwarding for a host on the network if it is not in the x.x.x.0 network. **Workaround:** None

Issues Carried over from Release 1.1.1.06

Number	Description
CSCul70357	System Summary page does not display the LAN interface IPv6 address. **Workaround:** None
CSCuf25163	iPhones, iPads, and iPods have difficulty establishing a VPN tunnel for EZVPN split mode. **Workaround:** Use EZVPN full tunnel mode.
CSCuf24407	SSL VPN clients are unable to access the HTTP/HTTPs service when the device is behind NAT. **Workaround:** None
CSCui00878	Remote Desktop Protocol (RDP) does not work through an SSL VPN tunnel on Windows 8. **Workaround:** None

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