Release Notes for Cisco RV34xx Router up to Firmware Version up to 1.0.03.28

Contents

This document includes the following topics:

Cisco RV34xx Router Firmware Version 1.0.03.28

Release date July 2022

This document describes resolved issues and known issues in Cisco RV340/ RV345/RV345P/RV340W Firmware Version 1.0.03.28. 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.

Most common configuration settings from the older firmware releases are supported on the new firmware version and are kept intact after upgrading. However, for optimal performance we recommend resetting the device to factory default settings, and rebuilding the configuration to accommodate any feature or firmware behavior changes.

IMPORTANT NOTE

A new firmware installation verification mechanism is optimized to reject invalid images. DO NOT downgrade the Firmware from 1.0.03.28 to 1.0.03.24 or other earlier versions.
If you really want to downgrade, select inactive version (1.0.03.24 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.

What's New

- Update ASDv3 to ASDv4 (this is a backend change only).
- Moved the DHCP-NAK option to new GUI menu.
- IPV6 LAN UI improvement.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.28

Number	Description
CSCwb35747	RV34x: IPv6 router advertisements sometimes set router lifetime to 0 when prefix delegation is used.
CSCwa67235	RV34x: Inbound IPv6 traffic does not pass to the host with ACL explicit allow.
CSCwc41905	Updated a few logs severity level.

Known Issues

The following table lists the resolved issues in firmware 1.0.03.28

Number	Description
CSCwc50260	IPv6 ACL doesn't work properly when WAN type is PPPoE with PD option.

Cisco RV34xx Router Firmware Version 1.0.03.27

Release date May 2022

This document describes resolved issues and known issues in Cisco RV340/ RV345/RV345P/RV340W Firmware Version 1.0.03.27. 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.

Most common configuration settings from the older firmware releases are supported on the new firmware version and are kept intact after upgrading. However, for optimal performance we recommend resetting the device to factory default settings, and rebuilding the configuration to accommodate any feature or firmware behavior changes.

IMPORTANT NOTE

A new firmware installation verification mechanism is optimized to reject invalid images. DO NOT downgrade the Firmware from1.0.03.27 to 1.0.03.24 or other earlier versions.
If you really want to downgrade, select inactive version (1.0.03.24 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.

What's New

Added DHCP NAK option to bypass the Server-ID check for specific scenarios.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.27

Number	Description
CSCwa72089	Can not apply the configurations sometimes.
CSCvz96100	RV34x router DHCP custom option to bypass NAK processing for the specific scenario.
CSCwa72211	Failed to provision the configuration file on rv34x by PnP.
CSCwa85645	RV34x: IPv6 DNS Servers missing prefix when using PD and DNS Proxy.
CSCwa71839	IKEv2 S2S issues Keep-alive issue: S2S tunnel only attempts to negotiate once. IKEv2 S2S issues: PSK with backslash.
CSCwa46246	RV34x: Service Auth Sequence secondary method changed by un-checking and then checking the Use Default button info.

Number	Description
CSCwa59921	RV340: post-auth command injection vulnerability in Cisco RV340 (usmUserPrivKey).
CSCwa59943	RV34x: A post-auth command injection vulnerability in Cisco RV340 (usmUserAuthKey).
CSCwa64992	RV340 JSON RPC set-snmp Stack-based Buffer Overflow RCE vulnerability (usmUserAuthKey).
CSCwa64996	RV340 JSON RPC set-snmp Stack-based Buffer Overflow RCE vulnerability (usmUserEngineID).
CSCwa64998	RV340 JSON RPC set-snmp Stack-based Buffer Overflow RCE vulnerability (usmUserPrivKey).
CSCwa37678	UCI Config Primary Certificate Command Injection vulnerability.

Known Issues

The following table lists the known issues in firmware 1.0.03.27

Number	Description
CSCwb33372	After downgrading to v1.0.03.26, you can't import config exported from v1.0.03.27. **Workaround** The new parameter 'dhcp-nak' is added in new version but not supported in old version. Search the dhcp-nak line in xml config: for “<dhcp-nak xmls=“http://cisco.com/ns/ciscosb/wan-ip”>false</dhcp-nak>”, and then delete the line. Now it can be imported successfully.

Cisco RV34xx Router Firmware Version 1.0.03.26

Release date January 2022

This document describes resolved issues and known issues in Cisco RV340/ RV345/RV345P/RV340W Firmware Version 1.0.03.26. 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.

Most common configuration settings from the older firmware releases are supported on the new firmware version and are kept intact after upgrading. However, for optimal performance we recommend resetting the device to factory default settings, and rebuilding the configuration to accommodate any feature or firmware behavior changes.

Known Issues

The following table lists the known issues in firmware 1.0.03.26

Number	Description
CSCwa72112	Firmware downgrade issue when using an external radius server. **Workaround** Export the configuration file, reset the device to factory default settings, then import the configuration back in.
CSCwa72211	Failed to provision the configuration file on RV34X by PnP.
CSCwa72089	Unable to apply configurations sometimes. **Workaround** Select “RADIUS”, “Local DB” or “other” option in the Service Authentication Sequence table. Do not select the “None” option.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.26

Number	Description
CSCvu99151	RV340W: Optimized Wireless instability and disconnect issues, and add more logs.
CSCvx79468	Optimize RV345 switch port stability.
CSCvz09655	DDNS may show a “disabled” status even though it is enabled and working properly.
CSCwa73870	RV34x: Seeing messages about freeing old Local DB memory.
CSCvz48525	RV34x: After importing the PKCS#12 file, some certs don’t show up in the list.
CSCwa04438	RV34x: Static NAT allows multiple entries to the same internal address.
CSCwa12732	Cisco Small Business RV Series Routers Upload Module Command Injection vulnerability.
CSCwa12748	Cisco Small Business RV Series Routers Digital Signature Verification Bypass vulnerability.
CSCwa12836	Cisco Small Business Routers Privilege Escalation vulnerability.
CSCwa13205	Cisco Small Business RV Series Routers SSL Certificate Validation vulnerability.
CSCwa13836	Cisco RV340/RV340W/RV345/RV345P Dual WAN Gigabit VPN Routers: SSL VPN Remote Code execution.
CSCwa13882	Cisco RV340/RV340W/RV345/RV345P Dual WAN Gigabit VPN Routers: Arbitrary File Upload.
CSCwa13888	Cisco RV340/RV340W/RV345/RV345P Dual WAN Gigabit VPN Routers: Arbitrary File Overwrite.
CSCwa13900	Cisco RV340/RV340W/RV345/RV345P Dual WAN Gigabit VPN Routers: Command Injection vulnerability.
CSCwa14008	Cisco Small Business RV Series Routers Open Plug N Play Command Injection vulnerability.

Number	Description
CSCwa14565	Cisco Small Business Routers Privilege Escalation vulnerability.
CSCwa14602	Cisco Small Business Routers Improper Session Management vulnerability.
CSCwa15168	Cisco Small Business Routers Privilege Escalation vulnerability.
CSCwa18770	Cisco Small Business RV Series Routers Upload Module Remote Code Execution vulnerability.
CSCwa32432	Cisco Small Business Routers Improper Session Management vulnerability.
CSCws36774	Cisco Small Business RV Series Routers File Copy Module Command Injection vulnerability.

Cisco RV34xx Router Firmware Version 1.0.03.24

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.24

Number	Description
CSCvy83972	RV34x: Email “Username” field does not accept entries longer than 32 characters.
CSCvw16972	RV34x: L2TP/IPSec user can’t access the server across S2S VPN.
CSCvy84001	RV34x: Email fails with “the server sent an empty reply” entry into the log.
CSCuy78144	Traffic from L2TP over IPSec to IPSec VPN is abnormal.
CSCvu95133	RV345: LAN status is showing all ports down/red even though it passes traffic.

Number	Description
CSCvy98424	RV345/RV345P: Some http/https web pages could not be opened with PPPoE tagged sub-interface.
CSCvy72894	RV340W: Can't browse to wireless section in GUI using Safari.
CSCvz98517	SQL Application not functional over RV34x S2S VPN.
CSCvz03980	RV340x: Enhancement request - option to disable security updates if not using the feature.

Cisco RV34xx Router Firmware Version 1.0.03.22

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.22

Number	Description
CSCvx36281	Cisco RV34x Dual WAN Gigabit VPN Routers Local Privilege Escalation Vulnerability.
CSCvy02178	New CDP memory leak vulnerability.
CSCvy15286	Cisco RV34x Dual WAN Gigabit VPN Routers Web Management RCE and DoS Vulnerability.
CSCvy15342	Cisco RV34x Dual WAN Gigabit VPN Routers Web Management Command Injection Vulnerability
CSCvw95017	Cisco Small Business RV Series Routers Link Layer Discovery Protocol Vulnerabilities.

Cisco RV34xx Router Firmware Version 1.0.03.21

Known Issues

The following table lists the known issues in firmware 1.0.03.21

Number	Description
CSCvx92617	The HUAWEI E3372 dongle may not work for some SP's 4G network. **Workaround** Suggest the customer to not upgrade if using this dongle.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.21

Number	Description
CSCvp94049	Novatel USB730L dongle shows as not connected on an RV340.
CSCvs59130	RV345P: ARP table showing incorrect 'Type' entries.
CSCvs61566	RV34x: Router ignores static route if it is part of a connected network.
CSCvv25800	RV34x: Router rejects radius accept message from Duo Server.
CSCvv71709	RV345P: Safari browser does not show the correct time.
CSCvw32986	RV34x: Router allows assigning x.x.x.0/24 address to VLAN.
CSCvw37657	RV34x: Slow speeds through router when AV is enabled.
CSCvw55469	RV34x: Can't remove the HW DMZ configuration info.
CSCvv83239	Multiple Vulnerabilities in dnsmasq DNS Forwarder Affecting Cisco Products: January 2021.
CSCvw62416	Cisco Small Business RV Series Routers Link Layer Discovery Protocol Vulnerabilities
CSCvw62418	Cisco Small Business RV Series Routers Link Layer Discovery Protocol Vulnerabilities
CSCvw92538	Cisco Small Business RV Series Routers Vulnerabilities
CSCvw92718	Cisco Small Business RV Series Routers Vulnerabilities
CSCvw94030	Cisco RV340/RV340W/RV345/RV345P VPN Routers Authenticated RCE Vulnerabilities.
CSCvw94062	Cisco RV340/RV340W/RV345/RV345P VPN Routers Authenticated RCE Vulnerabilities.
CSCvw94083	Cisco RV340/RV340W/RV345/RV345P VPN Routers Authenticated RCE Vulnerabilities.
CSCvw95017	Cisco Small Business RV Series Routers Link Layer Discovery Protocol Vulnerabilities.

Number	Description
CSC97341	RV340/RV340 Unauthenticated download vulnerability.

Cisco RV34xx Router Firmware Version 1.0.03.20

Release date October 2020

This document describes resolved issues and known issues in Cisco RV340/ RV345/RV345P/RV340W Firmware Version 1.0.03.28. 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.

What's New

- GUI optimization for the ARP Table and DHCP Bindings pages.
- Additional debug logs in the Tech Report file.
- Updated Online Help.
- Security signature update to 2.0.0.0013.

Known Issues

The following table lists the known issues in firmware 1.0.03.20

Number	Description
CSCvu54452 RV345P	After upgrading 1.0.02.16 to 1.0.03.16 or .17 back up config then restore fails. **Workaround** There are three classifier rules which have changed names in firmware versions 1.0.03.16 and newer. To correct this in configuration backup files, open the configuration file (version 1.0.03.16 or higher) using an XML or text editor and perform the following operations:: Change <name> SIP-TCP to <name> SIP_TCP Change <name> SIP-UDP to <name> SIP_UDP Change <name> SIP-RTP to <name> SIP_RTP Please note that your configuration file may not have all of theses sections. If one is not included in your configuration file, move to the next substitution. Save the updated configuration file and perform the restore on your device.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.20

Number	Description
CSCvu40103	OS command Injection in upload.cgi.
CSCvv59815	RV34x: CSR Details don't show all the fields entered.
CSCvu76240	RV34x: DNS-O-MATIC login failure.
CSCvs05534	RV34x: Traffic to router doesn't work if Site-to-Site VPN uses supernet of local network.
CSCvr01961	Network logs flooded with warning dnsmasq: ignoring nameserver 127.0.0.1.
CSCvs05528	RV34x: Error creating Site-to-Site VPN when remote network is supernet of local network
CSCvt39805	Evaluation of RV34x for pppd buffer overflow vulnerability

Cisco RV34xx Router Firmware Version 1.0.03.18

Release date July 2020

This section describes resolved issues and known issues in Cisco RV34xx Firmware Version 1.0.03.18.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.18

Number	Description
CSCvu36543	Cisco RV340 SSLVPN Pre Auth Remote Heap Overflow
CSCvu36544	Cisco RV340 SSLVPN Pre Auth Remote Null Pointer Dereference

Cisco RV34xx Router Firmware Version 1.0.03.17

Release date March 2020

This section describes resolved issues and known issues in Cisco RV34xx Firmware Version 1.0.03.17.

What's New

- Update ASDv2 to ASDv3
- Update security binary to improve stability

Known Issues

The following table lists the known issues in firmware 1.0.03.17

Number	Description
CSCvt29005	VPN auto loaded local ASN1DN on GUI is different from cert subject name. **Workaround** Use the certificate subject name from Administration > Certificate > Details when configuring IPSec VPN local/remote identifier for ASN1DN type.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.17

Number	Description
CSCvs87875	Evaluation of RV340W for Kr00k attack - CVE-2019-15126
CSCvr26531	RV34x: Disabling Inter VLAN Routing for a VLAN only blocks traffic to that VLAN.
CSCvo60322	RV34x: Router freezes - LAN traffic affected
CSCvs00049	RV34x After reboot or power cycle. Teleworker VPN UI status is incorrect.
CSCvp21416	SNMP returns identical values for in vs. out for some interface statistics.

Number	Description
CSCvn89322	Request for SNMP OID to monitor WAN/LAN ports be static.
CSCvo67683	Hardware DMZ can't work after reboot.
CSCvr79104	RV34x: Router slows or freezes when Security Services are enabled.
CSCvs40885	RV345 - Customer is seeing CPU spikes and slow performance when the Anti-virus is enabled.
CSCvo14530	(Rv340 request timed outW) SNMP WALK
CSCvq02081	Daylight Savings doesn't accept 'Last Week' as an option
CSCvr78163	Edit Teleworker VPN client button 'Apply' is disabled until few 'password' symbols are removed.
	Multi-WAN interface is showing offline state.
	Security signature updating by ASD fails.
	Unable to establish a S2S IKEv1 tunnel with ASN1DN for Local-ID & Remote-ID.
	DUT is generating continuous "Pe-Sync-Stop" errors when we establish Teleworker-VPN-client tunnel.

Cisco RV34xx Router Firmware Version 1.0.03.16

Release date August 2019

What's New

The IP Source Guard behavior is enhanced for the RV345. All of the IP/MAC entries in the user defined binding table and DHCP lease table will be protected if the IP source guard is enabled. There is no need to add entries

from the DHCP lease table to IP & MAC binding table.

- Supports dual image failover mechanism
- ASD enhancements

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.16

Number	Description
CSCvp48476	[RV340] “New firmware applied” alert always popups at login.
CSCvp72308	VLAN1 device management was disabled after firmware upgrade from v1.0.1.17 to v1.03.15.
CSCvp67501	RV34x: Teleworker VPN loses DNS information after a while.
CSCvq95133	WiFi driver update to improve wireless client connectivity.
CSCvp77132	RV34x: Full filename is not visible when down loading from USB.
CSCvp27090	RV34x: Email server password issue when using more than 15 characters for the password.
CSCvo14217	RV340W: Issue with one way audio when enabling WiFi calling service from the carrier.
CSCvp12551	RV34x: FTP Data channel fails on HW DMZ.
CSCvp01703	NAT hairpin doesn't work when the inter VLAN routing is disabled.
CSCvp35036	RV340-K9-G5: Huawei E3372 dongle stopped working after firmware upgrade.
CSCvp82450	Cisco RV340 Unwanted software embedded: GNU Debugger (gdb).
CSCvp75216	Cisco RV340 Series router static credentials vulnerability
CSCvq31953	Evaluation of rv34x for TCP SACK vulnerabilities.
CSCvp82418	Cisco RV340 Hard-coded password hashes

Number	Description
CSCvp73955	Evaluate Cisco RV34x for CVE-2015-7547 vulnerabilities

Cisco RV34xx Router Firmware Version 1.0.03.15

Release date April 2019

What's New

- Supports IPS/Antivirus and status
- Supports Multi-WAN detection status on system summary page
- Supports IKEv2 Non RFC compliant option.
- Supports IPSec global enable/disable option
- Removes AnyConnect from the Smart license. By default it supports 50 tunnels for the AnyConnect VPN.
- Able to edit the Cisco account in the Wizard after resetting device to factory default settings.
- Add option to customize web filtering block message.
- Allows to select the 3rd party certificate as primary certificate.
- Expanded the static NAT range length to 50.
- IPv6 PD configuration flow improvement with automatic setting for when the prefix is changed by SP.
- New PnP agent version which corrects the DNS related issue.
- Other GUI menus, options, GUI texts improvements.
- Supports DHCP settings in the VLAN configuration page.

Known Issues

The following table lists the known issues in firmware 1.0.03.15

Number	Description
CSCvp01703	RV34x: NAT hairpinning doesn't work when the InterVLAN Routing is disabled. **Workaround** Create firewall access rule to permit the traffic to the particular LAN server.
CSCvp28671	DUT assigns the wrong IPv6 DNS address when the IPv6 PD function is enabled. **Workaround** Assign a fixed DNS server address as a DNS proxy.
CSCvo57459	RV34x: Can't change the pre-shared key for L2TP/IPSec. **Workaround** None.
CSCvo11150	Sometimes the Host Name column in the DHCP bindings table is blank. **Workaround** None.
CSCvn25722	Wireless instability causing disconnections. **Workaround** Reboot or power cycle the router.
CSCvn09577	RV34x: Licensing is unregistered and the licenses are reset after the upgrade, if the default VLAN address is not 192.168.1.1. **Workaround** None. Need to re-register the license if your LAN address is different from 192.168.1.1.
CSCvk56283	DUT does not support loading configuration/firmware files with NTFS/exFAT format USB device. **Workaround** Use the FAT or FAT32 format.
CSCvm38989	Web filter device and OS type disappear after an image upgrade from 1.0.01.x to 1.0.02.x. **Workaround** If you configured the device/OS type before upgrading, you will need to reconfigure them in the IP Group objects after the upgrade.

Resolved Issues

The following table lists the resolved issues in firmware 1.0.03.15

Number	Description
CSCvn07210	DHCP option 43 IOT issue with the SMB switch.
CSCvn44878	IKEv2 S2S tunnel can not work with ASA.
CSCvn09537	RV34x: VPN Passthrough settings are reset on firmware upgrade.
CSCvm95735	After the reboot the DUT still displays off-line client info.
CSCvk43183	IKEv2 multiple subnets IOT with ISR router does not works properly.
CSCvg24303	RV34x: Add ability to view CPU and Memory information in system summary page.
CSCvo20003	The VPN traffic can't be forwarded by the DUT after running some time.
CSCvo76794	RV34x: Can't generate a CSR or Self-Signed Certificate with hyphen in Certificate Name.
CSCvo76859	RV34x: Importing Certificate fails if there is a hyphen in the certificate name.
CSCvo30111	RV34x: Can't add 1.0.0.0 network in the split-tunnel list.

Cisco RV34xx Router Firmware Version 1.0.02.16

Release date January 2019

What's New

- Cisco Umbrella feature
- IKEv2 support for Site-to-Site VPN and Client-to-Site VPN.
- Support Cisco PnP
- DNS-o-matic DDNS support
- Provide technical support report for troubleshooting purpose
- Support Option 43 on LAN DHCP server
- Linux kernel migrated with almost all drivers/ packages updated.
- Wireless ESDK migrated
- Support application control statistics and client statistics
- IP address group enhancements with device/OS types.
- Custom authentication sequence
- Support WAN single PPPoE session for IPOv4 and IPv6 connection
- Web filtering URL lookup
- GRE configuration flow improvements
- Support configurable remote syslog server port
- Support 3rd party CA certificates
- Support configurable web login session timeout
- New GUI style, along with GUI menus and options changes

Known Issues

The following table lists the known issues in firmware 1.0.02.16

Number	Description
CSCvn25722	Wireless instability causing disconnections. **Workaround** Reboot or power cycle the router.
CSCvn09577	RV34x: Licensing is unregistered and the licenses are reset after the upgrade, if the default VLAN address is not 192.168.1.1. **Workaround** None. Need to re-register the license if your LAN address is different from 192.168.1.1.
CSCvn09537	VPN Passthrough settings are reset on upgrade. **Workaround** Enable the VPN passthrough options manually after upgrading.
CSCvm95735	After a reboot, the client statistics display as offline clients with 0.0.0.0, until these same clients renew their addresses. **Workaround** None.
CSCvm89532	Keep the same AnyConnect VPN count after firmware upgrade. **Workaround** Manually update the AnyConnect VPN count in the license page after upgrading.
CSCvk56283	DUT does not support loading configuration/firmware files with NTFS/exFAT format USB device. **Workaround** Use the FAT or FAT32 format.
CSCvk43183	IKEv2 multiple subnets IOT with the ISR router does not work properly. **Workaround** None.

Number	Description
CSCvm38989	Web filter device and OS type disappear after an image upgrade from 1.0.01.x to 1.0.02.x. **Workaround** If you configured the device/OS type before upgrading, you will need to reconfigure them in the IP Group objects after the upgrade.
CSCvn01818	RV340: Dual WAN ports use IPv4 IP addresses from same subnet are allowed. **Workaround** None.
CSCvn44878	IKEv2 S2S tunnel can not work with ASA **Workaround** None.

Resolved Issues

The following table lists the resolve issues in firmware 1.0.02.16

Number	Description
CSCvj50141	RV34x: AnyConnect randomly stops working.
CSCvc40139	MU-MIMO reloads while running the performance testing with a fatal error log output.
CSCvd39976	SSID name that includes a space character are identified as two SSIDs in the group setting page.
CSCvd25865	IPv6 status displays as down when the IPv6 WAN type is PPPoE.
CSCvd34215	Two ASD processes in the backend which leads to failure when updating the firmware.
CSCvj24649	RV34x: Router does not accept DNS IP x.x.x.255
CSCvj83724	RV34x: ACL and Time Schedule is not working properly on the latest firmware 1.0.01.
CSCvj84327	RV340W: Fatal Error: wl1: wlc_dpc HAMMERING: MI_GPO set.

Number	Description
CSCvk05937	RV34x - After firmware upgrade, the web interface may not respond.
CSCvk20512	RV34x: Site to Site VPN tunnel/ netbios broadcast is not working
CSCvk39696	RV34x: disabled option Firewall - SIP ALG is allowing SIP ALG after unit reboot.
CSCvk76711	RV34x: When the WAN PPPoE interface is being used, the IPv6 cannot be disabled.
CSCvm20607	Client-to-site VPN on the WAN2 interface can't find xauth peer configuration through the FQDN
CSCvm50180	RV340W does not respond to SNMP polling action.
CSCvj31766	RV34x: Router freezes intermittently - WAN suspected
CSCvj41094	RV34x: VPN stops passing traffic intermittently

Cisco RV34xx Router Firmware Version 1.0.02.15

Release date November 2018

Known Issues

The following table lists the known issues in firmware 1.0.02.15

Number	Description
CSCvn09577	RV34x: Licensing is unregistered and the licenses are reset after the upgrade, if the default VLAN address is not 192.168.1.1. **Workaround** None. Need to re-register the license if your LAN address is different from 192.168.1.1.
CSCvn09537	VPN Passthrough settings are reset on upgrade. **Workaround** Enable the VPN passthrough options manually after upgrading.

Number	Description
CSCvm95735	After a reboot, the client statistics display as offline clients with 0.0.0.0, until these same clients renew their addresses. **Workaround** None.
CSCvm89532	Keep the same AnyConnect VPN count after firmware upgrade. **Workaround** Manually update the AnyConnect VPN count in the license page after upgrading.
CSCvk56283	DUT does not support loading configuration/firmware files with NTFS/exFAT format USB device. **Workaround** Use the FAT or FAT32 format.
CSCvk43183	IKEv2 multiple subnets IOT with the ISR router does not work properly. **Workaround** None.
CSCvm38989	Web filter device and OS type disappear after an image upgrade from 1.0.01.x to 1.0.02.x. **Workaround** If you configured the device/OS type before upgrading, you will need to reconfigure them in the IP Group objects after the upgrade.
CSCvn01818	RV340: Dual WAN ports use IPv4 IP addresses from same subnet are allowed. **Workaround** None.
CSCvn44878	IKEv2 S2S tunnel can not work with ASA **Workaround** None.

Resolved Issue

The following table lists the resolved issues in firmware 1.0.02.15

Number	Description
CSCvm66202	RV34x: Network Service Detection failure causes loss of Internet connectivity.
CSCvj50141	RV34x: AnyConnect randomly stops working.
CSCvc40139	MU-MIMO reloads while running the performance testing with a fatal error log output.
CSCvd39976	SSID name that includes a space character are identified as two SSIDs in the group setting page.
CSCvd25865	IPv6 status displays as down when the IPv6 WAN type is PPPoE.
CSCvd34215	Two ASD processes in the backend which leads to failure when updating the firmware.
CSCvj24649	RV34x: Router does not accept DNS IP x.x.x.255
CSCvj83724	RV34x: ACL and Time Schedule is not working properly on the latest firmware 1.0.01.
CSCvj84327	RV340W: Fatal Error: wl1: wlc_dpc HAMMERING: MI_GPO set.
CSCvk05937	RV34x - After firmware upgrade, the web interface may not respond.
CSCvk20512	RV34x: Site to Site VPN tunnel/ netbios broadcast is not working
CSCvk39696	RV34x: disabled option Firewall - SIP ALG is allowing SIP ALG after unit reboot.
CSCvk76711	RV34x: When the WAN PPPoE interface is being used, the IPv6 cannot be disabled.
CSCvm20607	c2s VPN on WAN2 interface can't find xuath peer config through FQDN
CSCvm50180	RV340W does not respond to SNMP polling action.

Cisco RV34xx Router Firmware Version 1.001.20

Release date October 2018

Resolved Issues

The following table lists the resolved issues in firmware 1.001.20

Number	Description
CSCvj07087	Removed the false positive log <alert>poemon: PoE VOP drift detected.
CSCvj24649	Router GUI does not accept DNS IP x.x.x.255.

Cisco RV34xx Router Firmware Version 1.001.18

Release date July 2018

What's New

In the 1.0.01.18 firmware release, a feature was introduced to enable/disable the device Management per VLAN. This feature is causing an issue in some of the devices and a patch will be released in the next firmware upgrade.

Currently the default factory loaded firmware version is 1.0.0.33. When you upgrade the router directly to 1.0.01.18 you will see the issue. Assuming this issue happens during fresh out-of-box start, then you must reset the router to factory default to fix it.

In firmware version 1.0.01.18, the default VLAN1 "Device Management" option will always be enabled and cannot be edited. When the device is upgraded from firmware .0.33 to .firmware 01.18, we observed that VLAN1 "Device Management" is disabled and cannot be changed to enabled.

The problem will be seen after upgrading the router under the following conditions:

Q. Can I use the single VLAN if the VLAN1 default IP is 192.168.1.0/24?

You can access the router, but you will notice that the VLAN1 "Device Management" is disabled.

Q. What if the VLAN1 default IP address is not 192.168.1.0/24 address?

Then, you will not be able to access the user interface.

Q. What happens when after an upgrade, the end-user changes the VLAN1 network address.

You will not be able to access the user interface.

Q. What happens if the router is configured with multiple VLANs?

You will not be able to access the user interface.

Steps for successful upgrade from 1.0.0.33

STEP 1 Back up the router's configuration before taking any action.

STEP 2 Upgrade the router to firmware version 1.0.01.17

STEP 3 Access the router from user interface.

STEP 4 Enable remote management (will be used for back door entry). This can be removed after successful firmware upgrade).

STEP 5 Save the running configuration to startup.

STEP 6 If Step 4 is not required because the remote access is already configured, then repeat step 5 to save your configuration with firmware version 1.0.1.17.

STEP 7 Upgrade the router's firmware to version 1.0.01.18.

STEP 8 Access the router from the LAN.

Steps for successful upgrade from 1.0.01.16 or 1.0.01.17

STEP 1 Always back up the configuration before taking any action.

STEP 2 Repeat steps 3-8.

Known Issues

The following table lists the known issues in firmware 1.001.18

Number	Description
CSCve80862	SNMP/syslog does not work over the VPN tunnel if the VPN remote subnet is configured as “Any”. **Workaround** Configure the VPN remote subnet with a specific subnet. Or, the User can add a specific route under “Routing -> static routing -> IPv4” using the SNMP agent host as the destination network address, mask 255.255.255.255, and “<NON-existent LAN host IP which falls into tunnel’s local subnet>” as the next hop, and the interface as the appropriate LAN interface (such as VLAN1). This route ensures that the reply traffic from the RV34X will be tunneled..
CSCvd39976	A SSID name that included a space character is identified as two SSIDs in the User Group setting page. **Workaround** Remove the special character from the SSID name.
CSCve55189	RV340W fails to save the running configuration to startup configuration. It becomes abnormal, after creating 10 captive portal profiles with 10 background pictures. **Workaround** Too many new pictures will occupy the configuration space. Please limit the captive portal profiles to less than 5 if you have to upload new pictures to each profile. Press the reset button for 10 seconds to reset to factory settings if the issue occurred.
CSCvd25865	IPv6 status shows that it is down when the IPv6 WAN type is PPPoE and IPv4 type is DHCP or static. **Workaround** Ignore the IPv6 status. If both IPv4 and IPv6 are PPPoE, the status is correct.

Number	Description
CSCvd17343	SNMP system uptime value is not the same as the device web GUI. **Workaround** None.
CSCvd34369	Can not connect to the Teleworker VPN Client manually. **Workaround** Enable the Auto Initiation Retry. It will connect/reconnect automatically in the backend. Or, choose “Do not Activate the Connection” before applying, then click the connect button.
CSCvd34360	Teleworker VPN Client IOT issue with ASA and RV325. **Workaround** Enable the PFS (Perfect Forward Secrecy) option on the ASA device.
CSCva62803	AC340U sometimes can not dial a connection on the USB1. **Workaround** Try the USB2 port and unplug and replug the dongle again.

Resolved Issues

The following table lists the resolved issues in firmware 1.001.18

Number	Description
CSCvg55169	RV34x: Router provides DHCP addresses when the DHCP server is disabled.
CSCvg94597	RV34x: S2S VPN status shows up but stops passing traffic.
CSCvf80775	RV34X: Pre-shared key shown in clear text in the router's log.
CSCvf25351	RV34x: VPN doesn't work when the DMZ Host is configured.
CSCvf94125	Wrong MDFID and SWTID in Bonjour for the RV340W and RV345.
CSCvg74957	Allow to disable IPv6 on the WAN interface

Number	Description
CSCvg62258	RV34x: User configuration issues when User Group name has a space in the name.
CSCvf45093	RV34x: Can't restrict web access for VLANs
CSCve91854	RV34x: Web filtering doesn't work if the URL has "_" in the address.
CSCve19873	Option82 cause win7/win10 client to send offer continuously.
CSCvd09880	RV34x: Reply to option3 info when option82 is enabled.

Cisco RV34xx Router Firmware Version 1.0.00.33

Release date September 2017

Known Issues

The following table lists the known issues in firmware 1.0.00.33

Number	Description
CSCva62803	AC340U sometimes can not dial a connection on the USB1. **Workaround** Try the USB2 port and unplug and replug the dongle again.
CSCva76883	SSLVPN is unable to startup when the client domain or login banner is blank. **Solution:** Input text on the login banner and client domain textbox.
CSCvb01361	Web filter: visit to website is slow when the web filter rule is added. **Workaround** None.

Number	Description
CSCvb21635	Router does not support EAP with a tagged packet. **Workaround** None.
CSCvb41417	IPSec VPN tunnel not up if setup with wizard and the DPD is enabled. **Workaround** None.
CSCvb49638	RIP thru GRE function not working. **Workaround** None.
CSCvb53431	Option82: Users have to enter hex string instead of ASCII string. **Workaround** None.
CSCvb65908	Content filter does not work when the allow list is empty. **Solution:** Input the websites that are allowed access and don't leave the table empty.
CSCvb65950	Static DHCP entry name which contain space character cause the DHCP process to stop. **Solution:** Do not use space character in the name.
CSCvb72529	DUT executes multi-processes of upgrade at the same time. **Solution:** Do not start ASD downloading multiple times. If it already happens, reboot the device and download again.
CSCvb76395	PPPoe user name can not accept "@" and "." in the setup wizard. **Solution:** Configure them on the GUI>WAN page instead of the wizard.
CSCvb80062	GUI Firefox: page has no response when edit expand category in AVC. **Solution:** Use Chrome browser.

Number	Description
CSCvb83781	RV345LAN switch ports LED/Link work abnormally intermittently. **Solution:** It happens very randomly. Reboot the device once it happens.
CSCvb83800	RV345/P WAN1 port can not forward traffic intermittently. **Solution:** It happens very randomly on some specific device. Reboot the device once it happens.
CSCvc52112	AVC: BB2 does not close http connection to webroot server when the server sends TCP FIN. **Solution:** None.
CSCvb88966	PPPoE connection can not be up sometimes. **Solution:** Plug out and plug in the WAN cable to make it work.

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 hash 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