Release Notes for Cisco RV0xx Dual WAN VPN Router Firmware Version 4.2.3.14

June 2020

These Release Notes describe the resolved issues in Cisco RV0xx Dual WAN VPN Router firmware version 4.2.3.14. The Cisco RV016 and RV082 have reached End of Life.

Resolved Issues

Issues Resolve in Firmware Version 4.2.3.14.

Ref Number	Description
CSCvt29372	Cisco Small Business RV Series Routers Command Injection Vulnerabilities.
CSCvt29376	Cisco Small Business RV Series Routers Command Injection Vulnerabilities.
CSCvt29381	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29385	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29388	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29396	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29398	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution

Ref Number	Description
CSCvt29400	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29403	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29405	Cisco Small Business RV Series Routers Command Injection Vulnerabilities
CSCvt29407	Cisco Small Business RV Series Routers Command Injection Vulnerabilities
CSCvt29409	Cisco Small Business RV Series Routers Command Injection Vulnerabilities
CSCvt29414	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29415	Cisco Small Business RV Series Routers Command Injection Vulnerabilities
CSCvt29416	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29421	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt29423	Cisco Small Business RV Series Routers Stack Overflow Arbitrary Code Execution
CSCvt39795	Evaluation of rv0xxv3 for pppd buffer overflow vulnerability

Issues Resolved in Firmware Version 4.2.3.10

Ref Number	Description
CSCvq34370	Static certificate and keys.
CSCvq34376	Static password hashes.
CSCvq3496	DNS mask vulnerabilities.
CSCvq34412	OpenSSL vulnerabilities.
CSCvq34415	UPnP vulnerabilities.
CSCvq76840	Weak cookies in web interface.
CSCvq76771	Hard-coded auth_key.
CSCvq97028	Critical command execution on the Cisco RV042/RV042G router.
CSCvq97031	Critical command execution on the Cisco RV082 router.
CSCvq95596	Critical command execution on the Cisco RV016 router.

Issues Resolved Firmware Version 4.2.3.09

Ref Number	Description
CSCvk56058	Configuration lost unexpectedly.

Issues Resolved in Firmware Version 4.2.3.08

Ref Number	Description
CSCvb81527	SSL certificate only supports SHA1.

Related Information

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport

Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Products. No login is required.
Product Documentation	
RV016	www.cisco.com/go/RV016
RV042	www.cisco.com/go/RV042
RV042G	www.cisco.com/go/RV042G
RV082	www.cisco.com/go/RV082
Cisco Small Business	
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb