Release Notes for Cisco RV130x Router up to Firmware Version 1.0.3.55

June 2020

This document describes known and resolved issues in the Cisco RV130x Firmware Version 1.0.3.55

Contents

Resolved Issues

Issues Resolved in Release 1.0.3.55

Number	Description
CSCvt28203	Cisco RV130W Router Command Injection Vulnerability
CSCvt28229	Cisco RV130W Routers Stack Overflow Vulnerability
CSCvt39798	Evaluation of rv130x for pppd buffer overflow vulnerability

Issues Resolved in Release 1.0.3.54

Number	Description
CSCvs87871	Evaluation of rv130x for Kr00k attack - CVE-2019-15126

Issues Resolved in Release 1.0.3.52

Number	Description
CSCvq31948	Evaluation of RV130x for TCP SACK vulnerabilities.

Issues Resolved in Release 1.0.3.51

Number	Description
CSCvo21850	Cisco RV130 web management interface buffer overflow.
CSCvo65034	Unauthenticated access to the syslog via the HTTP interface.
CSCvo65045	A remote unauthenticated attacker can remove stations on the guest network.
CSCvo65058	A remote unauthenticated attacker can acquire a list of all connected devices.

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

OL-25562-01