CVE-2019-1663

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-1663
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-28 18:29:00 UTC
Updated	2020-10-05 20:27:00 UTC
Description	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wi

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Rv110w	-	All	All	All
Hardware	Cisco	Rv110w	-	All	All	All
Operating System	Cisco	Rv110w Firmware	All	All	All	All
Operating System	Cisco	Rv110w Firmware	All	All	All	All
Hardware	Cisco	Rv130w	-	All	All	All
Hardware	Cisco	Rv130w	-	All	All	All
Operating System	Cisco	Rv130w Firmware	All	All	All	All
Operating System	Cisco	Rv130w Firmware	All	All	All	All
Hardware	Cisco	Rv215w	-	All	All	All
Hardware	Cisco	Rv215w	-	All	All	All
Operating System	Cisco	Rv215w Firmware	All	All	All	All
Operating System	Cisco	Rv215w Firmware	All	All	All	All

References

Reference	Source	Link
Cisco RV130W Routers - Management Interface Remote Command Execution (Metasploit) - Hardware remote Exploit	EXPLOIT-DB	www
Cisco RV130W Routers Management Interface Remote Command Execution	MISC	www

Cisco RV130W 1.0.3.44 Remote Stack Overflow ≈ Packet Storm	MISC	pack
Cisco RV110W, RV130W, and RV215W Routers Management Interface Remote Command Execution Vulnerability	CISCO	tools
Cisco RV110W / RV130(W) / RV215W Remote Command Execution ≈ Packet Storm	MISC	pack
Cisco RV130W Routers Management Interface Remote Command Execution ≈ Packet Storm	MISC	pack
Cisco RV110W/RV130W/RV215W Routers CVE-2019-1663 Remote Command Execution Vulnerability	BID	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.