

CVE-2019-1652

Cisco Small Business Routers Improper Input Validation Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Public exploit module (Metasploit)

A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker with administrative privileges on an affected device to execute arbitrary commands. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious HTTP POST requests to the web-based management interface of an affected device.

EVRS 83/100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.959 99.88th percentile · FIRST	CISA DEADLINE Mar 17, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.959 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux shell as root. Cisco has released firmware updates that address this vulnerability.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
rv320 firmware	≥ 1.4.2.15 < 1.4.2.22	1.4.2.22	NVD
rv325 firmware	≥ 1.4.2.15 < 1.4.2.22	1.4.2.22	NVD
rv320	–	no fixed version listed	NVD
rv325	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-73jm-6x85-hwg5

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject

NVD nvd.nist.gov/vuln/detail/CVE-2019-1652

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-10209

Current data evulnable.com/vulnerability-management/cve/CVE-2019-1652

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.