

CVE-2022-20700

Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.057 92.9th 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	0.057 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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

Affected and fixed versions · 10 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
rv340 firmware	≤ 1.0.03.24	after 1.0.03.24	NVD
rv340w firmware	≤ 1.0.03.24	after 1.0.03.24	NVD
rv345 firmware	≤ 1.0.03.24	after 1.0.03.24	NVD
rv345p firmware	≤ 1.0.03.24	after 1.0.03.24	NVD
rv160 firmware	≤ 1.0.01.05	after 1.0.01.05	NVD
rv160w firmware	≤ 1.0.01.05	after 1.0.01.05	NVD
rv260 firmware	≤ 1.0.01.05	no fixed version listed	NVD
rv260p firmware	≤ 1.0.01.05	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4jrj-gxg8-2frj**Additional guidance** tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D**NVD** nvd.nist.gov/vuln/detail/CVE-2022-20700**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2022-25950**Current data** evulnable.com/vulnerability-management/cve/CVE-2022-20700

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