

CVE-2018-0125

Cisco VPN Routers Remote Code Execution Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

A vulnerability in the web interface of the Cisco RV132W ADSL2+ Wireless-N VPN and RV134W VDSL2 Wireless-AC VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code and gain full control of an affected system, including issuing commands with root privileges. The attacker could also cause an affected system to reload, resulting in a denial of service (DoS) condition.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.552 99.03rd percentile · FIRST	CISA DEADLINE Apr 15, 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	0.552 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

The vulnerability is due to an incomplete input validation on user-controlled input in an HTTP request to the targeted device. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user and gain full control of the affected system or cause it to reload, resulting in a DoS condition. This vulnerability is fixed in firmware version 1.0.1.11 for the following Cisco products: RV132W ADSL2+ Wireless-N VPN Router and RV134W VDSL2 Wireless-AC VPN Router. Cisco Bug IDs: CSCvg92737, CSCvh60170.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
rv132w firmware	1.0	no fixed version listed	NVD
rv134w firmware	1.0	no fixed version listed	NVD
rv132w	–	no fixed version listed	NVD
rv134w	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4g9c-v6g6-3jgm

NVD nvd.nist.gov/vuln/detail/CVE-2018-0125

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-0948

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-rv13x
cisa.gov/known-exploited-vulnerabilities-catalog

CISA KEV
Current data evulnable.com/vulnerability-management/cve/CVE-2018-0125

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