



# CVE-2019-1652

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-1652
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-24 15:29:00 UTC
<b>Updated</b>	2020-10-05 19:34:00 UTC
<b>Description</b>	A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN

## Risk And Classification

**EPSS:** 0.927270000 probability, percentile 0.997600000 (date 2026-05-15)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-17; ransomware use Unknown

**Problem Types:** CWE-78

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers
<b>Name</b>	Cisco Small Business Routers Improper Input Validation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2019-1652">https://nvd.nist.gov/vuln/detail/CVE-2019-1652</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Cisco</a>	<a href="#">Rv320</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Rv320</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Rv320 Firmware</a>	1.4.2.15	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Rv320 Firmware</a>	1.4.2.15	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Rv325</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">Rv325</a>	-	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Rv325 Firmware</a>	1.4.2.15	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Rv325 Firmware</a>	1.4.2.15	All	All	All

## References

Reference	Source	Link
Cisco RV320 and RV325 - Unauthenticated Remote Code Execution (Metasploit) - Hardware remote Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
Cisco RV320 / RV325 Unauthenticated Remote Code Execution ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>
Cisco RV320 Command Injection ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>
Bugtraq: [RT-SA-2019-005] Cisco RV320 Command Injection Retrieval	BUGTRAQ	<a href="http://seclists.org">seclists.org</a>
Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability	CISCO	<a href="http://tools.cisco.com">tools.cisco.com</a>
Cisco RV320 Dual Gigabit WAN VPN Router 1.4.2.15 - Command Injection - Hardware webapps Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
Cisco RV320 and RV325 Routers CVE-2019-1652 Remote Command Injection Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Full Disclosure: [RT-SA-2019-005] Cisco RV320 Command Injection Retrieval	FULLDISC	<a href="http://seclists.org">seclists.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://CVE.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)