



# CVE-2019-15271

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-15271
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-26 03:15:00 UTC
<b>Updated</b>	2019-12-11 16:27:00 UTC
<b>Description</b>	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an attacker to exploit a deserialization of untrusted data (CWE-502) vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers. This vulnerability could allow an attacker to execute arbitrary code on the affected devices. The vulnerability is caused by the application's failure to properly validate and sanitize user input before deserializing it. The vulnerability is present in the following versions of the affected devices: RV016 Multi-wan Vpn, RV016 Multi-wan Vpn Firmware, RV042g Dual Gigabit Wan Vpn, and RV042g Dual Gigabit Wan Vpn Firmware. Cisco has released a security advisory (CVE-2019-15271) and a firmware update to address this vulnerability. Users are advised to apply the latest firmware update as soon as possible to their affected devices.

## Risk And Classification

**EPSS:** 0.056000000 probability, percentile 0.902890000 (date 2026-04-04)

**CISA KEV:** Listed on 2022-06-08; due 2022-06-22; ransomware use Unknown

**Problem Types:** CWE-502

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	RV Series Routers
<b>Name</b>	Cisco RV Series Routers Deserialization of Untrusted Data Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2019-15271">https://nvd.nist.gov/vuln/detail/CVE-2019-15271</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	<a href="#">Rv016 Multi-wan Vpn</a>	-	All	All	All
Hardware	Cisco	<a href="#">Rv016 Multi-wan Vpn</a>	-	All	All	All
Operating System	Cisco	<a href="#">Rv016 Multi-wan Vpn Firmware</a>	All	All	All	All
Operating System	Cisco	<a href="#">Rv016 Multi-wan Vpn Firmware</a>	All	All	All	All
Hardware	Cisco	<a href="#">Rv042g Dual Gigabit Wan Vpn</a>	-	All	All	All
Hardware	Cisco	<a href="#">Rv042g Dual Gigabit Wan Vpn</a>	-	All	All	All
Operating System	Cisco	<a href="#">Rv042g Dual Gigabit Wan Vpn Firmware</a>	All	All	All	All
Operating System	Cisco	<a href="#">Rv042g Dual Gigabit Wan Vpn Firmware</a>	All	All	All	All

Hardware	Cisco	Rv042 Dual Wan Vpn	-	All	All	All
Hardware	Cisco	Rv042 Dual Wan Vpn	-	All	All	All
Operating System	Cisco	Rv042 Dual Wan Vpn Firmware	All	All	All	All
Operating System	Cisco	Rv042 Dual Wan Vpn Firmware	All	All	All	All
Hardware	Cisco	Rv082 Dual Wan Vpn	-	All	All	All
Hardware	Cisco	Rv082 Dual Wan Vpn	-	All	All	All
Operating System	Cisco	Rv082 Dual Wan Vpn Firmware	All	All	All	All
Operating System	Cisco	Rv082 Dual Wan Vpn Firmware	All	All	All	All

## References

Reference	Source	Link
Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Arbitrary Command Execution Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.co</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[731377](#) Cisco Small Business RV (016,042,042G,082) Routers Arbitrary Command Execution Vulnerability (cisco-sa-20191106-sbrv-cmd-x)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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