



CVE-2022-27152

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

Summary

CVE	CVE-2022-27152
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-08 18:15:00 UTC
Updated	2023-08-29 22:15:00 UTC
Description	Roku devices running RokuOS v9.4.0 build 4200 or earlier that uses a Realtek WiFi chip is vulnerable to Arbitrary file modif

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Roku	Express	-	All	All	All
Hardware	Roku	Express 4k	-	All	All	All
Operating System	Roku	Roku Os	All	All	All	All
Hardware	Roku	Roku Tv	-	All	All	All
Hardware	Roku	Streambar	-	All	All	All
Hardware	Roku	Streambar Pro	-	All	All	All
Hardware	Roku	Streaming Stick 4k	-	All	All	All
Hardware	Roku	Streaming Stick 4k	-	All	All	All
Hardware	Roku	Ultra	-	All	All	All
Hardware	Roku	Wireless Speakers	-	All	All	All
Hardware	Roku	Wireless Subwoofer	-	All	All	All

References

Reference	Source	Link	Tags
Roku OS security updates	MISC	support.roku.com	
GitHub - llamasoft/RootMyRoku: A persistent root jailbreak for most Roku devices.	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report