



# CVE-2019-13209

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

## Summary

<b>CVE</b>	CVE-2019-13209
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-04 14:15:00 UTC
<b>Updated</b>	2022-04-13 23:44:00 UTC
<b>Description</b>	Rancher 2 through 2.2.4 is vulnerable to a Cross-Site Websocket Hijacking attack that allows an exploiter to gain access to

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Rancher</a>	<a href="#">Rancher</a>	All	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Rancher</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Latest Announcements topics - Rancher Labs	MISC	<a href="https://forums.rancher.com">forums.rancher.com</a>	Re
Rancher Release - v2.2.5 - Addresses Rancher CVE-2019-13209 - Announcements - Rancher Labs	CONFIRM	<a href="https://forums.rancher.com">forums.rancher.com</a>	Re
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[983829](#) Go (go) Security Update for github.com/rancher/rancher/server (GHSA-xhg2-rvm8-w2jh)

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](#)**