



# CVE-2021-38364

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

## Summary

<b>CVE</b>	CVE-2021-38364
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-20 13:15:00 UTC
<b>Updated</b>	2023-05-04 18:28:00 UTC
<b>Description</b>	An issue was discovered in ONOS 2.5.1. There is an incorrect comparison of flow rules installed by intents. A remote attack

## Risk And Classification

**Problem Types:** CWE-697

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Opennetworking</a>	<a href="#">Onos</a>	2.5.1	All	All	All

## References

Reference	Source	Link	Tags
Open Network Operating System (ONOS) SDN Controller for SDN/NFV Solutions	MISC	<a href="#">opennetworking.org</a>	
<a href="#">www.usenix.org/system/files/sec23fall-prepub-285_kim-jiwon.pdf</a>	MISC	<a href="#">www.usenix.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

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

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