



# CVE-2022-0669

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

## Summary

<b>CVE</b>	CVE-2022-0669
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-29 15:15:00 UTC
<b>Updated</b>	2022-09-01 20:35:00 UTC
<b>Description</b>	A flaw was found in dpdk. This flaw allows a malicious vhost-user master to attach an unexpected number of fds as ancillar

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	All	All	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	19.11	All	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	19.11	rc1	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	19.11	rc2	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	19.11	rc3	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	19.11	rc4	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	22.03	rc1	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	22.03	rc2	All	All
Application	<a href="#">Dpdk</a>	<a href="#">Data Plane Development Kit</a>	22.03	rc3	All	All
Application	<a href="#">Openvswitch</a>	<a href="#">Openvswitch</a>	2.13.0	All	All	All
Application	<a href="#">Openvswitch</a>	<a href="#">Openvswitch</a>	2.15.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.0	All	All	All

## References

Reference	Source	Link
CVE-2022-0669	MISC	<a href="#">security-track</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat</a>

vhost: fix FD leak with inflight messages · DPDK/dpdk@af74f7d · GitHub	MISC	<a href="https://github.com">github.com</a>
922 – CVE-2022-0669 State: Confirmed (Issue in handling of vhost-user inflight type messages)	MISC	<a href="https://bugs.dpdk.org">bugs.dpdk.org</a>
2055793 – (CVE-2022-0669) CVE-2022-0669 dpdk: sending vhost-user-inflight type messages could lead to DoS	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</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>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [179268](#) Debian Security Update for dpdk (DSA 5130-1)
- [182072](#) Debian Security Update for dpdk (CVE-2022-0669)
- [198772](#) Ubuntu Security Notification for DPDK Vulnerabilities (USN-5401-1)
- [672077](#) EulerOS Security Update for dpdk (EulerOS-SA-2022-2254)
- [672079](#) EulerOS Security Update for dpdk (EulerOS-SA-2022-2241)
- [672084](#) EulerOS Security Update for dpdk (EulerOS-SA-2022-2284)
- [672133](#) EulerOS Security Update for dpdk (EulerOS-SA-2022-2313)
- [752291](#) SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:2273-1)
- [753440](#) SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:1892-1)

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

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