CVE-2022-2132

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-2132
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 16:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	A permissive list of allowed inputs flaw was found in DPDK. This issue allows a remote attacker to cause a denial of service

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Dpdk	Data Plane Development Kit	All	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Enterprise Linux Fast Datapath	7.0	All	All	All
Application	Redhat	Enterprise Linux Fast Datapath	8.0	All	All	All
Application	Redhat	Enterprise Linux Fast Datapath	9.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	S
1031 – CVE-2022-2132	M
[SECURITY] [DLA 3092-1] dpdk security update	M

2099475 – (CVE-2022-2132) CVE-2022-2132 dpdk: DoS when a Vhost header crosses more than two descriptors and exhausts all mbufs	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 160307 Oracle Enterprise Linux Security Update for dpdk (ELSA-2022-8263)
- 160397 Oracle Enterprise Linux Security Update for dpdk (ELSA-2023-0171)
- 180981 Debian Security Update for dpdk (DSA 5222-1)
- 180987 Debian Security Update for dpdk (DLA 3092-1)
- 183140 Debian Security Update for dpdk (CVE-2022-2132)
- 198933 Ubuntu Security Notification for DPDK Vulnerability (USN-5608-1)
- 240797 Red Hat Update for OpenStack Platform 13.0 (RHSA-2022:7268)
- 240900 Red Hat Update for dpdk (RHSA-2022:8263)
- 241065 Red Hat Update for dpdk (RHSA-2023:0169)
- 241066 Red Hat Update for dpdk (RHSA-2023:0172)
- 241067 Red Hat Update for dpdk (RHSA-2023:0171)
- 241068 Red Hat Update for dpdk (RHSA-2023:0170)
- 241069 Red Hat Update for dpdk (RHSA-2023:0167)
- 241639 Red Hat Update for dpdk (RHSA-2023:0168)
- 241672 Red Hat Update for dpdk (RHSA-2023:0166)
- 377903 Alibaba Cloud Linux Security Update for dpdk (ALINUX3-SA-2023:0009)
- 672369 EulerOS Security Update for dpdk (EulerOS-SA-2022-2761)
- 672383 EulerOS Security Update for dpdk (EulerOS-SA-2022-2726)
- 672414 EulerOS Security Update for dpdk (EulerOS-SA-2022-2793)
- 672435 EulerOS Security Update for dpdk (EulerOS-SA-2022-2843)
- 672445 EulerOS Security Update for dpdk (EulerOS-SA-2022-2818)
- 752610 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3356-1)
- 752620 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3381-1)

752629 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3430-1)

752630 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3429-1)

753388 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3341-1)

753435 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022:3390-1)

755779 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2024:0529-1)

755785 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2024:0531-1)

755786 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2024:0530-1)

755796 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2024:0554-1)

755813 SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2024:0576-1)

940804 AlmaLinux Security Update for dpdk (ALSA-2022:8263)

940883 AlmaLinux Security Update for dpdk (ALSA-2023:0171)

960527 Rocky Linux Security Update for dpdk (RLSA-2023:0171)

960601 Rocky Linux Security Update for dpdk (RLSA-2022:8263)

© 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 registred 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