



CVE-2023-4459

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

Summary

CVE	CVE-2023-4459
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-21 19:15:00 UTC
Updated	2024-03-13 15:15:00 UTC
Description	A NULL pointer dereference flaw was found in vmxnet3_rq_cleanup in drivers/net/vmxnet3/vmxnet3_drv.c in the networking

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
cve-details	MISC	access.rec
RHSA-2024:1250		access.rec
Red Hat		access.rec
net: vmxnet3: fix possible NULL pointer dereference in vmxnet3_rq_cle... · torvalds/linux@edf410c · GitHub	MISC	github.com
RHSA-2024:1306		access.rec
2219268 – (CVE-2023-4459) CVE-2023-4459 kernel: vmxnet3: NULL pointer dereference in vmxnet3_rq_cleanup()	MISC	bugzilla.re
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160949](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12842)

[199765](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6388-1)

[242855](#) Red Hat Update for kernel (RHSA-2024:0412)

[243050](#) Red Hat Update for kernel (RHSA-2024:1250)

[243062](#) Red Hat Update for kernel-rt (RHSA-2024:1306)

[243076](#) Red Hat Update for kernel (RHSA-2024:1367)

[243096](#) Red Hat Update for kernel-rt (RHSA-2024:1382)

[390290](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2023-0023)

[673449](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2898)

[673484](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3033)

[673563](#) EulerOS Security Update for kernel (EulerOS-SA-2024-1144)

[673732](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3010)

[673848](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3217)

[673970](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2879)

[754832](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3600-1)

[754833](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3599-1)

[754855](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3656-1)

[754863](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3680-1)

[754866](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3684-1)

[754867](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3683-1)

[754868](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3682-1)

[754869](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3681-1)

[754876](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3687-1)

[754883](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3705-1)

[754884](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3704-1)

[754899](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3599-2)

[754900](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3600-2)

[754901](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3704-2)

754903 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3683-2)
755026 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3964-1)
755037 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3971-1)
755038 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3969-1)
755043 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3988-1)

© [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](#) 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](#)