



# CVE-2022-4744

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

## Summary

<b>CVE</b>	CVE-2022-4744
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-30 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:58:00 UTC
<b>Description</b>	A double-free flaw was found in the Linux kernel's TUN/TAP device driver functionality in how a user registers the device w

## Risk And Classification

**Problem Types:** CWE-415

## 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	Linux	Linux Kernel	5.16	rc7	All	All

## References

Reference	Source	Link	Tags
CVE-2022-4744 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] [DLA 3403-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CentOS Stream 9 Missing Kernel Security Fix ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
kernel/git/netdev/net.git - Netdev Group's networking tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160524](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-1470)

[161147](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)

<a href="#">181687</a> Debian Security Update for linux (CVE-2022-4744)
<a href="#">181768</a> Debian Security Update for linux (DLA 3403-1)
<a href="#">241293</a> Red Hat Update for kpatch-patch (RHSA-2023:1471)
<a href="#">241295</a> Red Hat Update for kernel-rt (RHSA-2023:1469)
<a href="#">241296</a> Red Hat Update for kernel-rt (RHSA-2023:1467)
<a href="#">241297</a> Red Hat Update for kernel security (RHSA-2023:1468)
<a href="#">241298</a> Red Hat Update for kernel security (RHSA-2023:1470)
<a href="#">241299</a> Red Hat Update for kpatch-patch (RHSA-2023:1466)
<a href="#">242434</a> Red Hat Update for kernel-rt security (RHSA-2023:6901)
<a href="#">242451</a> Red Hat Update for kernel security (RHSA-2023:7077)
<a href="#">243087</a> Red Hat Update for kernel (RHSA-2024:1404)
<a href="#">354904</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-044
<a href="#">378468</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
<a href="#">378512</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
<a href="#">378710</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
<a href="#">673393</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
<a href="#">674113</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
<a href="#">753902</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:1800-1)
<a href="#">753905</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:1811-1)
<a href="#">755851</a> SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)
<a href="#">940966</a> AlmaLinux Security Update for kernel (ALSA-2023:1470)
<a href="#">940967</a> AlmaLinux Security Update for kernel-rt (ALSA-2023:1469)
<a href="#">941453</a> AlmaLinux Security Update for kernel (ALSA-2023:7077)
<a href="#">960891</a> Rocky Linux Security Update for kernel-rt (RLSA-2023:1469)
<a href="#">960896</a> Rocky Linux Security Update for kernel (RLSA-2023:1470)

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](#)**