



# CVE-2023-3567

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

## Summary

<b>CVE</b>	CVE-2023-3567
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-24 16:15:00 UTC
<b>Updated</b>	2024-01-30 17:15:00 UTC
<b>Description</b>	A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This issue may al

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	22.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc1	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc2	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc3	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc4	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc5	All	All
Operating System	Linux	Linux Kernel	6.2.0	rc6	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

## References

**Reference**

Patch "vc\_screen: move load of struct vc\_data pointer in vcs\_read() to avoid UAF" has been added to the 6.1-stable tree — Linux Stable Com

Red Hat

Red Hat

Kernel Live Patch Security Notice LSN-0099-1 ≈ Packet Storm

Red Hat

Red Hat

2221463 – (CVE-2023-3567) CVE-2023-3567 kernel: use after free in vcs\_read in drivers/tty/vt/vc\_screen.c due to race

Red Hat

Red Hat

cve-details

Kernel Live Patch Security Notice LSN-0098-1 ≈ Packet Storm

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[199775](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6341-1)

[242759](#) Red Hat Update for kernel (RHSA-2024:0432)

[242789](#) Red Hat Update for kernel (RHSA-2024:0575)

[242845](#) Red Hat Update for kernel (RHSA-2024:0448)

[242846](#) Red Hat Update for kernel-rt (RHSA-2024:0439)

[242847](#) Red Hat Update for kernel-rt (RHSA-2024:0431)

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

[356753](#) Amazon Linux Security Advisory for kernel : ALAS2-2023-2359

[356782](#) Amazon Linux Security Advisory for kernel : ALAS-2023-1897

[379043](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)

[379435](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)

[673354](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2843)

[673496](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2860)

[754275](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3309-1)

[754281](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:3349-1)

754829	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP3) (SUSE-SU-2023:3594-1)
754830	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 15 SP1) (SUSE-SU-2023:3596-1)
754831	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP3) (SUSE-SU-2023:3595-1)
754834	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 25 for SLE 15 SP3) (SUSE-SU-2023:3607-1)
754835	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 15 SP1) (SUSE-SU-2023:3603-1)
754838	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 38 for SLE 15 SP2) (SUSE-SU-2023:3622-1)
754839	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 15 SP2) (SUSE-SU-2023:3621-1)
754840	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 15 SP2) (SUSE-SU-2023:3620-1)
754841	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP3) (SUSE-SU-2023:3623-1)
754842	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 35 for SLE 15 SP2) (SUSE-SU-2023:3612-1)
754844	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 32 for SLE 15 SP3) (SUSE-SU-2023:3628-1)
754845	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP3) (SUSE-SU-2023:3627-1)
754846	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 34 for SLE 15 SP3) (SUSE-SU-2023:3632-1)
754847	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP3) (SUSE-SU-2023:3631-1)
754848	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2023:3630-1)
754854	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 8 for SLE 15 SP4) (SUSE-SU-2023:3644-1)
754873	SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2023:3671-1)

© [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](#)