



CVE-2023-0597

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-0597
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-23 20:15:00 UTC
Updated	2023-07-28 15:15:00 UTC
Description	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was found in the

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	6.2	rc1	All	All

References

Reference	Source	Link	Tags
oss-security - Re: StackRot (CVE-2023-3269): Linux kernel privilege escalation vulnerability	MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [161066](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)
- [161147](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)
- [199452](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6206-1)
- [199521](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6235-1)

199670 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6300-1)
199842 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6440-1)
199849 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6440-2)
199864 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6440-3)
199882 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6462-1)
199919 Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6462-2)
242399 Red Hat Update for kernel security (RHSA-2023:6583)
242434 Red Hat Update for kernel-rt security (RHSA-2023:6901)
242451 Red Hat Update for kernel security (RHSA-2023:7077)
243041 Red Hat Update for kernel security (RHSA-2024:1188)
283671 Fedora Security Update for kernel (FEDORA-2023-c9ab30c8e3)
283672 Fedora Security Update for kernel (FEDORA-2023-4006357f7e)
378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)
378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
378710 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
673121 EulerOS Security Update for kernel (EulerOS-SA-2023-2296)
673157 EulerOS Security Update for kernel (EulerOS-SA-2023-2272)
753801 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0762-1)
753806 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0770-1)
753807 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0768-1)
753808 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0778-1)
753810 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0780-1)
754023 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2232-1)
755842 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:0774-1)
755851 SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)
941453 AlmaLinux Security Update for kernel (ALSA-2023:7077)

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](#)