



CVE-2023-6606

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

Summary

CVE	CVE-2023-6606
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-08 17:15:00 UTC
Updated	2024-03-12 03:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	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	Tags
RHSA-2024:1248		access.redhat.com	
access.redhat.com/security/cve/CVE-2023-6606		access.redhat.com	Third Party Advisory
RHBZ#2253611		bugzilla.redhat.com	Exploit, Issue Tracking
lists.debian.org/debian-lts-announce/2024/01/msg00004.html		lists.debian.org	
RHSA-2024:0897		access.redhat.com	
RHSA-2024:0723		access.redhat.com	
bugzilla.kernel.org/show_bug.cgi		bugzilla.kernel.org	Exploit, Issue Tracking
RHSA-2024:0725		access.redhat.com	
RHSA-2024:1188		access.redhat.com	
RHSA-2024:0881		access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161372 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12169)
161402 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0897)
161417 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-1248)
200065 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6603-1)
200067 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6602-1)
200068 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6608-1)
200070 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6606-1)
200072 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6604-1)
200074 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6607-1)
200076 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6609-1)
200077 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6605-1)
200079 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6604-2)
200080 Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-6605-2)
200088 Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6609-2)
200096 Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6609-3)
200103 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-1)
200112 Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6608-2)
200113 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6635-1)
200118 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-2)
242887 Red Hat Update for kernel-rt (RHSA-2024:0725)
242908 Red Hat Update for kernel (RHSA-2024:0723)
242939 Red Hat Update for kernel (RHSA-2024:0897)
242983 Red Hat Update for kernel-rt (RHSA-2024:0881)
243041 Red Hat Update for kernel security (RHSA-2024:1188)
243052 Red Hat Update for kernel (RHSA-2024:1248)

243087 Red Hat Update for kernel (RHSA-2024:1404)
357014 Amazon Linux Security Advisory for kernel : ALAS2-2024-2418
357041 Amazon Linux Security Advisory for kernel : ALAS2023-2024-488
357044 Amazon Linux Security Advisory for kernel : ALAS-2024-1906
357050 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2024-034
357053 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2024-058
357054 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2024-046
357088 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-164
357092 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-162
357100 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-163
357109 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-161
357314 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-167
357318 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2024-169
6000429 Debian Security Update for linux (DLA 3710-1)
6140389 AWS Bottlerocket Security Update for kernel (GHSA-xf23-qjp2-xxhg)
673321 EulerOS Security Update for kernel (EulerOS-SA-2024-1337)
673547 EulerOS Security Update for kernel (EulerOS-SA-2024-1315)
673714 EulerOS Security Update for kernel (EulerOS-SA-2024-1196)
673723 EulerOS Security Update for kernel (EulerOS-SA-2024-1237)
673902 EulerOS Security Update for kernel (EulerOS-SA-2024-1176)
673992 EulerOS Security Update for kernel (EulerOS-SA-2024-1215)
673995 EulerOS Security Update for kernel (EulerOS-SA-2024-1275)
755604 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0129-1)
755605 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0120-1)
755606 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0117-1)
755607 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0115-1)
941584 AlmaLinux Security Update for kernel (ALSA-2024:0897)

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