



CVE-2023-34324

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

Summary

CVE	CVE-2023-34324
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-05 17:15:00 UTC
Updated	2024-01-05 18:23:00 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
XSA-441 - Xen Security Advisories		xenbits.xenproject.org	
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

[199881](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6461-1)

[200098](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6625-1)

[200099](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6624-1)

[200100](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6626-1)

[200102](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6625-2)

[200103](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-1)

[200111](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6626-2)

[200118](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6628-2)

[200120](#) Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6626-3)

200125 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-6625-3)
200132 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6652-1)
356562 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-055
356579 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-029
356598 Amazon Linux Security Advisory for kernel : ALAS2-2023-2328
356612 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-042
356634 Amazon Linux Security Advisory for kernel : ALAS2023-2023-422
356744 Amazon Linux Security Advisory for kernel : ALAS-2023-1883
6000419 Debian Security Update for linux (DSA 5594-1)
6000428 Debian Security Update for linux-5.10 (DLA 3711-1)
6000429 Debian Security Update for linux (DLA 3710-1)
6140065 AWS Bottlerocket Security Update for kernel (GHSA-3gq7-xph5-x9hv)
673714 EulerOS Security Update for kernel (EulerOS-SA-2024-1196)
755235 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4377-1)
755238 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4378-1)
755240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4375-1)
755249 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4414-1)
755563 SUSE Security Update for the linux kernel (SUSE-SU-2023:4351-1)
755564 SUSE Security Update for the linux kernel (SUSE-SU-2023:4348-1)
755565 SUSE Security Update for the linux kernel (SUSE-SU-2023:4347-1)
755566 SUSE Security Update for the linux kernel (SUSE-SU-2023:4345-1)
755567 SUSE Security Update for the linux kernel (SUSE-SU-2023:4343-1)

© [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](#)