



CVE-2023-2513

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

Summary

CVE	CVE-2023-2513
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-08 21:15:00 UTC
Updated	2023-11-07 04:12:00 UTC
Description	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for ex

Risk And Classification

Problem Types: CWE-416

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	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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
[PATCH v3 0/4] ext4: fix use-after-free in ext4_xattr_set_entry - Baokun Li		lore.kernel.org	
[PATCH v3 0/4] ext4: fix use-after-free in ext4_xattr_set_entry - Baokun Li	MISC	lore.kernel.org	
2193097 - (CVE-2023-2513) CVE-2023-2513 kernel: ext4: use-after-free in ext4_xattr_set_entry()	MISC	bugzilla.redhat.com	
ext4: fix use-after-free in ext4_xattr_set_entry · torvalds/linux@67d7d8a · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160949](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12842)

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

[181852](#) Debian Security Update for linux (CVE-2023-2513)

[199617](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6254-1)

[242434](#) Red Hat Update for kernel-rt security (RHSA-2023:6901)

[242451](#) Red Hat Update for kernel security (RHSA-2023:7077)

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

[355083](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-032

[355088](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-045

[355100](#) Amazon Linux Security Advisory for kernel : ALAS2-2023-2035

[355103](#) Amazon Linux Security Advisory for kernel : ALAS-2023-1744

[378701](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0030)

[390290](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2023-0023)

[6140081](#) AWS Bottlerocket Security Update for kernel (GHSA-q3wq-fc3p-vjrw)

[673288](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2631)

[673310](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2601)

[673393](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2647)

[674113](#) EulerOS Security Update for kernel (EulerOS-SA-2023-2689)

[754097](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2507-1)

[754105](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2537-1)

[754106](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2534-1)

[754110](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2538-1)

[754120](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2611-1)

[754145](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2651-1)

[755851](#) SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)

[906884](#) Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (26681-1)

[906947](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26689-1)

[906983](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (26682-1)

© [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](#)