



CVE-2023-37454

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

Summary

CVE	CVE-2023-37454
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-06 17:15:00 UTC
Updated	2023-11-07 04:16:00 UTC
Description	An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image causes a use-after-free write op

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

References

Reference	Source	Link
BUG: unable to handle kernel paging request in udf_close_lvid	MISC	syzkaller.a
[syzbot] KASAN: use-after-free Write in udf_close_lvid	MISC	lore.kernel
1213122 – (CVE-2023-37454) VUL-0: CVE-2023-37454: kernel: use-after-free write operation in the udf_put_super	MISC	bugzilla.su
[syzbot] KASAN: use-after-free Write in udf_close_lvid		lore.kernel
KASAN: use-after-free Write in udf_close_lvid	MISC	syzkaller.a
KASAN: use-after-free Write in udf_close_lvid	MISC	syzkaller.a
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)