



CVE-2021-3996

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

Summary

CVE	CVE-2021-3996
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 20:15:00 UTC
Updated	2024-01-07 09:15:00 UTC
Description	A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUS

Risk And Classification

Problem Types: CWE-552

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Kernel	Util-linux	All	All	All	All

References

Reference	Source	Link
snap-confine must_mkdir_and_open_with_perms() Race Condition ≈ Packet Storm	MISC	packetstormsecurity
libmount: remove support for deleted mount table entries · util-linux/util-linux@166e873 · GitHub	MISC	github.com
August 2022 Util-linux Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
2024628 – (CVE-2021-3996) CVE-2021-3996 util-linux: Unauthorized unmount of filesystems in libmount	MISC	bugzilla.redhat.com
mirrors.edge.kernel.org/pub/linux/utils/util-linux/v2.37/v2.37.3-ReleaseNotes	MISC	mirrors.edge.kernel.
Full Disclosure: Race condition in snap-confine's must_mkdir_and_open_with_perms() (CVE-2022-3328)	FULLDISC	seclists.org
oss-security - Race condition in snap-confine's must_mkdir_and_open_with_perms() (CVE-2022-3328)	MLIST	www.openwall.com
oss-security - CVE-2021-3996 and CVE-2021-3995 in util-linux's libmount	MISC	www.openwall.com
GLSA-202401-08		security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179023 Debian Security Update for util-linux (DSA 5055-1)
184614 Debian Security Update for util-linux (CVE-2021-3996)
198660 Ubuntu Security Notification for util-linux Vulnerabilities (USN-5279-1)
282338 Fedora Security Update for util (FEDORA-2022-9d02441b24)
354315 Amazon Linux Security Advisory for util-linux : ALAS2022-2022-086
354387 Amazon Linux Security Advisory for util-linux : ALAS2022-2022-099
354474 Amazon Linux Security Advisory for util-linux : ALAS2022-2022-218
354581 Amazon Linux Security Advisory for util-linux : ALAS-2022-218
355340 Amazon Linux Security Advisory for util-linux : ALAS2023-2023-024
376419 Snap-Confine Local Privilege Escalation Vulnerability (Oh Snap! More Lemmings)
500713 Alpine Linux Security Update for util-linux
504487 Alpine Linux Security Update for util-linux
6140047 AWS Bottlerocket Security Update for util-linux (GHSA-9fh2-79qc-65m6)
671444 EulerOS Security Update for util-linux (EulerOS-SA-2022-1461)
671460 EulerOS Security Update for util-linux (EulerOS-SA-2022-1440)
671640 EulerOS Security Update for util-linux (EulerOS-SA-2022-1654)
671644 EulerOS Security Update for util-linux (EulerOS-SA-2022-1668)
710828 Gentoo Linux util-linux Multiple Vulnerabilities (GLSA 202401-08)
751814 OpenSUSE Security Update for libeconf, shadow and util-linux (openSUSE-SU-2022:0727-1)
752028 SUSE Enterprise Linux Security Update for libeconf, shadow and util-linux (SUSE-SU-2022:0727-1)
903783 Common Base Linux Mariner (CBL-Mariner) Security Update for util-linux (10710)

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](#)