



# CVE-2022-33981

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

## Summary

<b>CVE</b>	CVE-2022-33981
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-18 16:15:00 UTC
<b>Updated</b>	2022-11-05 02:28:00 UTC
<b>Description</b>	drivers/block/floppy.c in the Linux kernel before 5.17.6 is vulnerable to a denial of service, because of a concurrency use-af

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.6">cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.6</a>	MISC	<a href="https://cdn.kernel.org">cdn.kernel.org</a>	
oss-sec: Linux kernel: A concurrency use-after-free in floppy's raw_cmd	MISC	<a href="https://seclists.org">seclists.org</a>	
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
floppy: disable FDRAWCMD by default · torvalds/linux@233087c · GitHub	MISC	<a href="https://github.com">github.com</a>	
IBM X-Force Exchange	MISC	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
[SECURITY] [DLA 3065-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160012](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9667)

[179385](#) Debian Security Update for linux (CVE-2022-33981)

[180282](#) Debian Security Update for linux (DLA 3065-1)

[180605](#) Debian Security Update for linux (DSA 5173-1)

[198857](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5514-1)

[198861](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5518-1)

[198875](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5539-1)

[198891](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5560-1)

[198897](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5564-1)

[377117](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)

[378043](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0011)

[390264](#) Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0021)

[672016](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2273)

[672139](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2428)

[672158](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2415)

[752340](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2377-1)

[752349](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2382-1)

[752354](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2393-1)

[752359](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2411-1)

[752360](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2407-1)

[752363](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2423-1)

[752364](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2422-1)

[752370](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)

[752391](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2549-1)

[752463](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2809-1)

[752911](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)

[752913](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)

[753038](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)

753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753148 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)
753271 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2424-1)
753362 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2376-1)
753703 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753707 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753727 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
902356 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9955)
902359 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9952)
902646 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9952-1)
902707 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9955-1)
905940 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9955-2)
906263 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9952-2)

© [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](#)**