



# CVE-2022-4379

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

## Summary

<b>CVE</b>	CVE-2022-4379
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-10 22:15:00 UTC
<b>Updated</b>	2023-06-26 16:55:00 UTC
<b>Description</b>	A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw allows an att

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc6	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc7	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1	rc8	All	All

## References

Reference	Source	Link	Tag
oss-sec: CVE-2022-4379: Linux kernel: use-after-free in __nfs42_ssc_open	MISC	<a href="#">seclists.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="#">git.kernel.org</a>	

[SECURITY] Fedora 37 Update: kernel-6.1.5-200.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: kernel-6.1.5-100.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
[SECURITY] [DLA 3404-1] linux-5.10 security update	MISC	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 37 Update: kernel-6.1.5-200.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: kernel-6.1.5-100.fc36 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [160490](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0951)
- [181765](#) Debian Security Update for linux-5.10 (DLA 3404-1)
- [182102](#) Debian Security Update for linux (CVE-2022-4379)
- [199207](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5914-1)
- [199208](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5915-1)
- [199209](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5912-1)
- [199210](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5913-1)
- [199211](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5911-1)
- [199220](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5929-1)
- [199223](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5935-1)
- [199227](#) Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5938-1)
- [199229](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5941-1)
- [199238](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5950-1)
- [199243](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5962-1)
- [241215](#) Red Hat Update for kernel-rt (RHSA-2023:0979)
- [241218](#) Red Hat Update for kernel (RHSA-2023:0951)
- [241229](#) Red Hat Update for kpatch-patch (RHSA-2023:1008)
- [241258](#) Red Hat Update for kernel security (RHSA-2023:1202)
- [241260](#) Red Hat Update for kernel-rt (RHSA-2023:1203)

<a href="#">241290</a> Red Hat Update for kpatch-patch (RHSA-2023:1435)
<a href="#">283611</a> Fedora Security Update for kernel (FEDORA-2023-f4f9182dc8)
<a href="#">283612</a> Fedora Security Update for kernel (FEDORA-2023-3fd7349f60)
<a href="#">354883</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-016
<a href="#">354885</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-029
<a href="#">355199</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
<a href="#">355354</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-126
<a href="#">355357</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-127
<a href="#">355362</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-125
<a href="#">378710</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
<a href="#">379043</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
<a href="#">6140360</a> AWS Bottlerocket Security Update for kernel (GHSA-4mw8-q274-9j97)
<a href="#">753564</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0147-1)
<a href="#">753565</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0146-1)
<a href="#">753584</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0149-1)
<a href="#">753623</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP4) (SUSE-SU-2023:0270-1)
<a href="#">753626</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 6 for SLE 15 SP4) (SUSE-SU-2023:0273-1)
<a href="#">753629</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 5 for SLE 15 SP4) (SUSE-SU-2023:0280-1)
<a href="#">753630</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2023:0277-1)
<a href="#">753660</a> SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2023:0320-1)
<a href="#">753662</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP4) (SUSE-SU-2023:0331-1)
<a href="#">905192</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (12946)
<a href="#">905231</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (12950)
<a href="#">905271</a> Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13020)
<a href="#">905282</a> Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13028)
<a href="#">906815</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (12946-1)
<a href="#">906874</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (12950-1)
<a href="#">940942</a> AlmaLinux Security Update for kernel (ALSA-2023:0951)

[940952](#) AlmaLinux Security Update for kernel-rt (ALSA-2023:0979)

[960667](#) Rocky Linux Security Update for kernel-rt (RLSA-2023:0979)

© [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](#)**