



# CVE-2023-3268

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

## Summary

<b>CVE</b>	CVE-2023-3268
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-16 19:15:00 UTC
<b>Updated</b>	2023-11-07 04:18:00 UTC
<b>Description</b>	An out of bounds (OOB) memory access flaw was found in the Linux kernel in relay_file_read_start_pos in kernel/relay.c in

## Risk And Classification

### Problem Types: CWE-125

## 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>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 3508-1] linux security update	MLIST	<a href="#">lists.debian.org</a>	
[PATCH] relayfs: fix out-of-bounds access in relay_file_read	MISC	<a href="#">lore.kernel.org</a>	
Debian -- Security Information -- DSA-5480-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
<a href="#">cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.3.2</a>	MISC	<a href="#">cdn.kernel.org</a>	
Debian -- Security Information -- DSA-5448-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
[PATCH] relayfs: fix out-of-bounds access in relay_file_read		<a href="#">lore.kernel.org</a>	
<a href="#">kernel/git/torvalds/linux.git - Linux kernel source tree</a>	MISC	<a href="#">git.kernel.org</a>	
CVE-2023-3268 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
[SECURITY] [DLA 3623-1] linux-5.10 security update	MLIST	<a href="#">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">161066</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)
<a href="#">161147</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)
<a href="#">199615</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6252-1)
<a href="#">199617</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6254-1)
<a href="#">199652</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6283-1)
<a href="#">199670</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6300-1)
<a href="#">199784</a> Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6397-1)
<a href="#">242399</a> Red Hat Update for kernel security (RHSA-2023:6583)
<a href="#">242434</a> Red Hat Update for kernel-rt security (RHSA-2023:6901)
<a href="#">242451</a> Red Hat Update for kernel security (RHSA-2023:7077)
<a href="#">242855</a> Red Hat Update for kernel (RHSA-2024:0412)
<a href="#">243050</a> Red Hat Update for kernel (RHSA-2024:1250)
<a href="#">243062</a> Red Hat Update for kernel-rt (RHSA-2024:1306)
<a href="#">355531</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-034
<a href="#">355532</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-021
<a href="#">355536</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-047
<a href="#">378701</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0030)
<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="#">6000136</a> Debian Security Update for linux (DLA 3508-1)
<a href="#">6000207</a> Debian Security Update for linux (DSA 5448-1)
<a href="#">6000212</a> Debian Security Update for linux (DSA 5480-1)
<a href="#">6000265</a> Debian Security Update for linux-5.10 (DLA 3623-1)
<a href="#">6140267</a> AWS Bottlerocket Security Update for kernel (GHSA-rgrv-2p2x-qfxw)

<a href="#">673261</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2614)
<a href="#">673272</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2584)
<a href="#">673354</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2843)
<a href="#">673372</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2787)
<a href="#">673496</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2860)
<a href="#">673498</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3132)
<a href="#">673604</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2811)
<a href="#">754160</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2808-1)
<a href="#">754167</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2822-1)
<a href="#">754168</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2830-1)
<a href="#">754170</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2834-1)
<a href="#">754183</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2859-1)
<a href="#">907115</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27222-1)
<a href="#">907173</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27248-1)
<a href="#">941453</a> AlmaLinux Security Update for kernel (ALSA-2023:7077)

© [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](#)**