



# CVE-2022-0494

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

## Summary

<b>CVE</b>	CVE-2022-0494
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-25 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:41:00 UTC
<b>Description</b>	A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw

## Risk And Classification

**Problem Types:** CWE-908

## 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>	9.0	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>	5.17	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.17	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.17	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.17	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.17	rc4	All	All

## References

Reference	Source	Link	T
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
2039448 - (CVE-2022-0494) CVE-2022-0494 kernel: information leak in scsi_ioctl()	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	
[PATCH] block-map: add __GFP_ZERO flag for alloc_page in function bio_copy_kern - Haimin Zhang		<a href="http://lore.kernel.org">lore.kernel.org</a>	
[PATCH] block-map: add __GFP_ZERO flag for alloc_page in function bio_copy_kern - Haimin Zhang	MISC	<a href="http://lore.kernel.org">lore.kernel.org</a>	
[SECURITY] [DLA 3065-1] linux security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	

Debian -- Security Information -- DSA-5161-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160039</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-6003)
<a href="#">160171</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7110)
<a href="#">179371</a> Debian Security Update for linux (DSA 5161-1)
<a href="#">180282</a> Debian Security Update for linux (DLA 3065-1)
<a href="#">180605</a> Debian Security Update for linux (DSA 5173-1)
<a href="#">184183</a> Debian Security Update for linux (CVE-2022-0494)
<a href="#">198747</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5381-1)
<a href="#">198891</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5560-1)
<a href="#">198895</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5562-1)
<a href="#">198911</a> Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5582-1)
<a href="#">199560</a> Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6001-1)
<a href="#">199568</a> Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6013-1)
<a href="#">199577</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6014-1)
<a href="#">240600</a> Red Hat Update for kernel-rt (RHSA-2022:6002)
<a href="#">240604</a> Red Hat Update for kernel security (RHSA-2022:6003)
<a href="#">240643</a> Red Hat Update for kernel-rt (RHSA-2022:6248)
<a href="#">240644</a> Red Hat Update for kernel (RHSA-2022:6243)
<a href="#">240776</a> Red Hat Update for kernel-rt (RHSA-2022:7134)
<a href="#">240782</a> Red Hat Update for kernel security (RHSA-2022:7110)
<a href="#">353960</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-014
<a href="#">353962</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-026
<a href="#">353976</a> Amazon Linux Security Advisory for kernel : ALAS-2022-1604
<a href="#">353985</a> Amazon Linux Security Advisory for kernel : ALAS2-2022-1813

<a href="#">354468</a> Amazon Linux Security Advisory for kernel : ALAS2022-2022-185
<a href="#">354499</a> Amazon Linux Security Advisory for kernel : ALAS2022-2022-042
<a href="#">354542</a> Amazon Linux Security Advisory for kernel : ALAS-2022-185
<a href="#">355199</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
<a href="#">377117</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)
<a href="#">377871</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)
<a href="#">6140117</a> AWS Bottlerocket Security Update for kernel (GHSA-48j3-m5cc-9vqw)
<a href="#">671804</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1844)
<a href="#">671862</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1896)
<a href="#">671870</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1934)
<a href="#">671929</a> EulerOS Security Update for kernel (EulerOS-SA-2022-1999)
<a href="#">671975</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2159)
<a href="#">672003</a> EulerOS Security Update for kernel (EulerOS-SA-2022-2134)
<a href="#">752370</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
<a href="#">753148</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)
<a href="#">900811</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9270)
<a href="#">901365</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9240)
<a href="#">902034</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9270-1)
<a href="#">902126</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9240-1)
<a href="#">905829</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9270-2)
<a href="#">906354</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9240-2)
<a href="#">940634</a> AlmaLinux Security Update for kernel (ALSA-2022:6003)
<a href="#">940637</a> AlmaLinux Security Update for kernel-rt (ALSA-2022:6002)
<a href="#">940709</a> AlmaLinux Security Update for kernel-rt (ALSA-2022:7134)
<a href="#">940719</a> AlmaLinux Security Update for kernel (ALSA-2022:7110)
<a href="#">960271</a> Rocky Linux Security Update for kernel-rt (RLSA-2022:7134)
<a href="#">960397</a> Rocky Linux Security Update for kernel (RLSA-2022:7110)

© [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](#)**