



# CVE-2023-3212

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

## Summary

<b>CVE</b>	CVE-2023-3212
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-23 20:15:00 UTC
<b>Updated</b>	2023-10-26 20:17:00 UTC
<b>Description</b>	A NULL pointer dereference issue was found in the gfs2 file system in the Linux kernel. It occurs on corrupt gfs2 file system

## Risk And Classification

**Problem Types:** CWE-476

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	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>	6.4	rc1	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

Operating System	Redhat	Enterprise Linux	9.0	All	All	All
------------------	--------	------------------	-----	-----	-----	-----

## References

Reference	Source	Link
gfs2: Don't deref jdesc in evict · torvalds/linux@504a10d · GitHub	MISC	<a href="https://github.com">github.com</a>
Debian -- Security Information -- DSA-5480-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
2214348 – (CVE-2023-3212) CVE-2023-3212 kernel: gfs2: NULL pointer dereference in gfs2_evict_inode()	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
CVE-2023-3212 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
Debian -- Security Information -- DSA-5448-1 linux	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 3623-1] linux-5.10 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

161066 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)
161147 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7077)
199469 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6231-1)
199757 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6339-4)
199765 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6388-1)
199783 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6396-1)
199804 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6417-1)
199810 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6412-1)
199812 Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-6396-2)
199834 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6396-3)
199883 Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6466-1)
242399 Red Hat Update for kernel security (RHSA-2023:6583)
242434 Red Hat Update for kernel-rt security (RHSA-2023:6901)
242451 Red Hat Update for kernel security (RHSA-2023:7077)
355864 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-051
356403 Amazon Linux Security Advisory for kernel : ALAS2-2023-2268

<a href="#">356578</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-054
<a href="#">378889</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0036)
<a href="#">378892</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0114)
<a href="#">379043</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
<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="#">6000429</a> Debian Security Update for linux (DLA 3710-1)
<a href="#">673354</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2843)
<a href="#">673496</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2860)
<a href="#">907075</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27328-1)
<a href="#">907167</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (27308-1)
<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](#)