



CVE-2023-40791

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

Summary

CVE	CVE-2023-40791
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-16 03:15:00 UTC
Updated	2024-01-04 19:08:00 UTC
Description	extract_user_to_sg in lib/scatterlist.c in the Linux kernel before 6.4.12 fails to unpin pages in a certain situation, as demonstr

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link	Tags
LKML: Yikebaer Aizezi: WARNING in try_grab_page	MISC	lkml.org	
cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.4.12	MISC	cdn.kernel.org	
[PATCH] crypto, cifs: Fix error handling in extract_iter_to_sg() - David Howells		lore.kernel.org	
[PATCH] crypto, cifs: Fix error handling in extract_iter_to_sg() - David Howells	MISC	lore.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	

CVE-2023-40791 Linux Kernel Vulnerability in NetApp Products NetApp Product Security		security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[907557](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31564-1)

© [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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report