



CVE-2023-5215

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

Summary

CVE	CVE-2023-5215
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-28 14:15:00 UTC
Updated	2024-01-03 19:03:00 UTC
Description	A flaw was found in libnbd. A server can reply with a block size larger than 2^63 (the NBD spec states the size is a 64-bit un

Risk And Classification

Problem Types: CWE-252

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Libnbd	All	All	All	All

References

Reference	Source	Link	Tags
2241041 – (CVE-2023-5215) CVE-2023-5215 libnbd: NBS server does not return expeted block size	MISC	bugzilla.redhat.com	
cve-details	MISC	access.redhat.com	
[Libguestfs] [libnbd PATCH v2 3/6] api: Sanitize sizes larger than INT64_MAX	MISC	listman.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[755171](#) SUSE Enterprise Linux Security Update for libnbd (SUSE-SU-2023:4222-1)

[907526](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libnbd (31095-1)

© [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](#)