



CVE-2011-1925

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

Summary

CVE	CVE-2011-1925
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-31 20:55:00 UTC
Updated	2023-11-07 02:07:00 UTC
Description	nbd-server.c in Network Block Device (nbd-server) 2.9.21 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted requests.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wouter Verhelst	Nbd	All	All	All	All

References

Reference	Source	Link	Tags
Gentoo Linux Documentation -- nbd: Multiple vulnerabilities	GENTOO	security.gentoo.org	
oss-security - CVE request: nbd-server	MLIST	www.openwall.com	
#627042 - security flaw in 2.9.21 - Debian Bug report logs	MISC	bugs.debian.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Network Block Device Server NULL Pointer Dereference Denial of Service Vulnerability	BID	www.securityfocus.com	
Network Block Device / Git tools		nbd.git.sourceforge.net	
Network Block Device / Git tools	CONFIRM	nbd.git.sourceforge.net	Patch
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)