



CVE-2009-2483

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

Summary

CVE	CVE-2009-2483
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-16 16:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	libprop/prop_object.c in proplib in NetBSD 4.0 and 4.0.1 allows local users to cause a denial of service (NULL pointer deref

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netbsd	Netbsd	4.0	All	All	All
Operating System	Netbsd	Netbsd	4.0.1	All	All	All
Operating System	Netbsd	Netbsd	4.0	All	All	All
Operating System	Netbsd	Netbsd	4.0.1	All	All	All

References

Reference	Source
55285	OSVDB
IBM X-Force Exchange	XF
NetBSD-SA2009-003	NETBSD
SecurityTracker.com Archives - NetBSD proplib Null Pointer Dereference in Processing XML Data Lets Local Users Deny Service	SECTRA
NetBSD proplib Undefined XML Element Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
NetBSD 'proplib' Library XML Processing Null Pointer Exception Denial Of Service Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)