



CVE-2005-4782

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

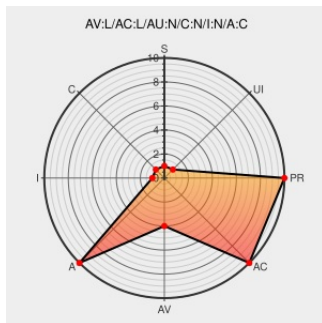
CVE-2005-4782

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Netbsd](#) from [Netbsd](#) contain the following vulnerability:

NetBSD 2.0 before 2.0.4, 2.1 before 2.1.1, and 3, when the kernel is compiled with "options DIAGNOSTIC," allows local users to cause a denial of service (kernel assertion panic) via a negative linger time in the SO_LINGER socket option.

CVE-2005-4782 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Patch
[cvsweb.netbsd.org](#)
text/x-diff

CONFIRM
[cvsweb.netbsd.org/bsdweb.cgi/src/sys/kern/uipc_socket.c.diff?r1=1.111&r2=1.112](#)

netbsd-announce: NetBSD Security Advisory 2005-012: SO_LINGER argument checking DIAGNOSTIC panic

Patch
[mail-index.netbsd.org](#)
text/html

NETBSD NetBSD-SA2005-012

NetBSD SO_LINGER DIAGNOSTIC Checking Local Denial of Service Vulnerability

[cve.report \(archive\)](#)
text/html

BID 15289

source-changes: CVS commit: src/sys/kern

Patch
[mail-index.netbsd.org](#)
text/html

MLIST [source-changes] 20051021 CVS commit: src/sys/kern

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

Readers are interested to get the information shared as external source or other sites being referenced, or not, from this page. There may be other resources that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netbsd	Netbsd	2.0	All	All	All
Operating System	Netbsd	Netbsd	2.0.1	All	All	All
Operating System	Netbsd	Netbsd	2.0.2	All	All	All
Operating System	Netbsd	Netbsd	2.0.3	All	All	All
Operating System	Netbsd	Netbsd	2.1	All	All	All
Operating System	Netbsd	Netbsd	2.0	All	All	All
Operating System	Netbsd	Netbsd	2.0.1	All	All	All
Operating System	Netbsd	Netbsd	2.0.2	All	All	All
Operating System	Netbsd	Netbsd	2.0.3	All	All	All
Operating System	Netbsd	Netbsd	2.1	All	All	All
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.1:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.2:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.3:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.1:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.1:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.2:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.0.3:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:2.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023   |

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](#)