



# CVE-2005-4783

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

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

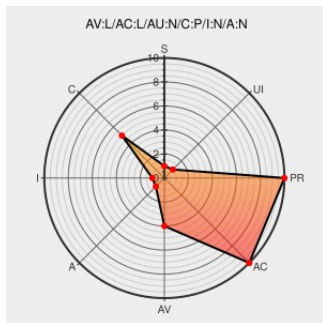
## CVE-2005-4783

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

kernfs\_xread in kernfs\_vnops.c in NetBSD before 20050831 does not check for a negative offset when reading the message buffer, which allows local users to read arbitrary kernel memory.

CVE-2005-4783 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

**Access Vector**

**LOCAL**

**Access Complexity**

**LOW**

**Authentication**

**NONE**

**Confidentiality Impact**

**PARTIAL**

**Integrity Impact**

**NONE**

**Availability Impact**

**NONE**

## CVE References

| Description                                            | Tags                                                                                              | Link                                                                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| netbsd-announce: Announcing update 2.0.3 - source only | <a href="#">mail-index.netbsd.org</a><br><a href="#">text/html</a>                                | <a href="#">MLIST [netbsd-announce] 20051031 Announcing update 2.0.3 - source only</a>                       |
| CVS log for src/sys/miscfs/kernfs/kernfs_vnops.c       | <a href="#">Patch</a><br><a href="#">cvsweb.netbsd.org</a><br><a href="#">text/html</a>           | <a href="#">CONFIRM</a><br><a href="#">cvsweb.netbsd.org/bsdweb.cgi/src/sys/miscfs/kernfs/kernfs_vnops.c</a> |
| <b>No Description Provided</b>                         | <a href="#">Patch</a><br><a href="#">www.osvdb.org</a>                                            | <a href="#">OSVDB 20729</a>                                                                                  |
|                                                        | <b>Inactive Link</b> <b>Not Archived</b>                                                          |                                                                                                              |
| Files ≈ Packet Storm                                   | <a href="#">Patch</a><br><a href="#">www.packetstormsecurity.org</a><br><a href="#">text/html</a> | <a href="#">NETBSD NetBSD-SA2006-001</a>                                                                     |
| src/sys/miscfs/kernfs/kernfs_vnops.c                   | <a href="#">Patch</a>                                                                             | <a href="#">CONFIRM</a>                                                                                      |

- diff - 1.111

[cvsweb.netbsd.org](http://cvsweb.netbsd.org)  
[text/html](#)

[cvsweb.netbsd.org/bsdweb.cgi/src/sys/miscfs/kernfs/kernfs\\_vnops.c.diff?r1=1.110&r2=1.111&f=h](https://cvsweb.netbsd.org/bsdweb.cgi/src/sys/miscfs/kernfs/kernfs_vnops.c.diff?r1=1.110&r2=1.111&f=h)

## SecurityTracker.com Archives - NetBSD Bugs in Kernel, Networking, and Application Code May Let Local Users Deny Service or Gain Elevated Privileges

```
Patch
securitytracker.com
text/html
```

 SECTRAK 1015132

404 Not Found

Patch  
releng.netbsd.org  
text/html  
Inactive Link Not Archived

 [CONFIRM releng.netbsd.org/cgi-bin/req-3.cgi?show=727](https://releng.netbsd.org/cgi-bin/req-3.cgi?show=727)

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 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](mailto: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 | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 1.6     | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.0     | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.0.3   | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.1     | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 1.6     | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.0     | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.0.3   | All    | All     | All      |
| Operating System | <a href="#">Netbsd</a> | <a href="#">Netbsd</a> | 2.1     | All    | All     | All      |

```
cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:netbsd:netbsd:2.0.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:netbsd:netbsd:2.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:netbsd:netbsd:2.0:*:*:*:*:*:*
```

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](#)