

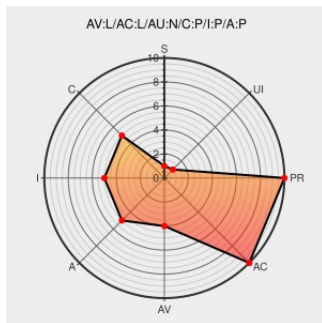


CVE-2004-0114

Published on: 03/03/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0114

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The shmat system call in the System V Shared Memory interface for FreeBSD 5.2 and earlier, NetBSD 1.3 and earlier, and OpenBSD 2.6 and earlier, does not properly decrement a shared memory segment's reference count when the vm_map_find function fails, which could allow local users to gain read or write access to a portion of kernel memory and gain privileges.

CVE-2004-0114 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

OpenBSD 3.3 errata

[www.openbsd.org](http://www.openbsd.org/text/html)
[text/html](http://www.openbsd.org/text/html)

CONFIRM
www.openbsd.org/errata33.html#sysvshm

Computest neemt Pine Digital Security over -
Computest

www.pine.nl
[text/plain](http://www.pine.nl/text/plain)

>> MISC www.pine.nl/press/pine-cert-20040201.txt

ftp.netbsd.org
[text/plain](http://ftp.netbsd.org/text/plain)

NETBSD NetBSD-SA2004-004

BSD Kernel SHMAT System Call Privilege
Escalation Vulnerability

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

BID 9586

'[PINE-CERT-20040201] reference count overflow in shmat()' - MARC

marc.info

text/html

BUGTRAQ 20040205 [PINE-CERT-20040201] reference count overflow in shmat()

No Description Provided

www.osvdb.org

Inactive Link

Not Archived

OSVDB 3836

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF bsd-shmat-gain-privileges(15061)

Patch

Vendor Advisory

ftp.freebsd.org

text/plain

Inactive Link

Not Archived

FREEBSD FreeBSD-SA-04:02

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Netbsd	Netbsd	All	All	All	All
Operating System	Openbsd	Openbsd	All	All	All	All

cpe:2.3:o:freebsd:freebsd:*.***.***.***:

cpe:2.3:o:netbsd:netbsd:*.***.***.***:

cpe:2.3:o:openbsd:openbsd:*.***.***.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →