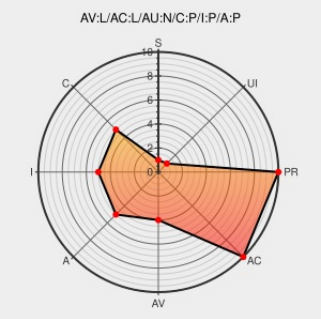
CVE-2004-0114

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
OpenBSD 3.3 errata	www.openbsd.org text/html	CONFIRM www.openbsd.org/errata33.html#sysvshm
Computest neemt Pine Digital Security over - Computest	www.pine.nl text/plain	>> MISC www.pine.nl/press/pine-cert-20040201.txt
	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

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→