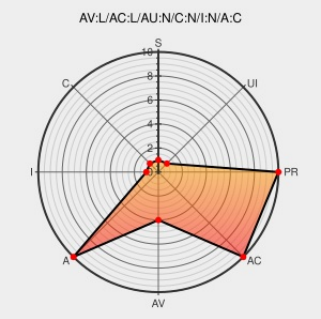
CVE-2006-1589

Published on: 04/03/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1589

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Netbsd from Netbsd contain the following vulnerability:

The elf_load_file function in NetBSD 2.0 through 3.0 allows local users to cause a denial of service (kernel crash) via an ELF interpreter that does not have a PT_LOAD section in its header, which triggers a null dereference.

CVE-2006-1589 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF netbsd-elfloadfile-dos(25690)
	Patch Vendor Advisory ftp.NetBSD.org text/plain	NETBSD NetBSD-SA2006-008
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24576
NetBSD elf_load_file() Validation Error Lets Local Users Crash the System - SecurityTracker	Patch securitytracker.com text/html	SECTRACK 1015848

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	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	3.0	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
Operating System	Netbsd	Netbsd	3.0	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:3.0:*:*:*:*:*:*:*:

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:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→