

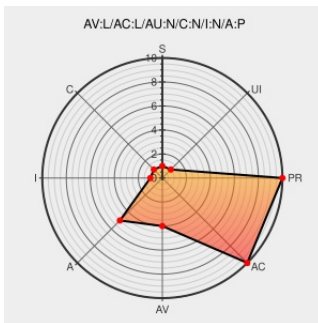


CVE-2002-1490

Published on: 04/02/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1490

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

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

NetBSD 1.4 through 1.6 beta allows local users to cause a denial of service (kernel panic) via a series of calls to the TIOCSCTTY ioctl, which causes an integer overflow in a structure counter and sets the counter to zero, which frees memory that is still in use by other processes.

CVE-2002-1490 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

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

[OSVDB 7566](#)

Inactive Link Not Archived

ISS X-Force Database: netbsd-tiocscctty-ioctl-bo (10115): NetBSD TIOCSCCTTY ioctl structure counter buffer overflow

Patch
Vendor Advisory
web.archive.org
text/html

[XF netbsd-tiocscctty-ioctl-bo\(10115\)](#)

Inactive Link Not Archived

ftp.netbsd.org
text/plain

[NETBSD
NetBSD-SA2002-007](#)

NetBSD Repeated TIOSCTTY IOCTL Buffer Overflow Vulnerability

Patch
Vendor Advisory

[BID 5722](#)

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	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.4	All	alpha	All
Operating System	Netbsd	Netbsd	1.4	All	arm32	All
Operating System	Netbsd	Netbsd	1.4	All	sparc	All
Operating System	Netbsd	Netbsd	1.4	All	x86	All
Operating System	Netbsd	Netbsd	1.4.1	All	All	All
Operating System	Netbsd	Netbsd	1.4.1	All	alpha	All
Operating System	Netbsd	Netbsd	1.4.1	All	arm32	All
Operating System	Netbsd	Netbsd	1.4.1	All	sh3	All
Operating System	Netbsd	Netbsd	1.4.1	All	sparc	All
Operating System	Netbsd	Netbsd	1.4.1	All	x86	All
Operating System	Netbsd	Netbsd	1.4.2	All	All	All
Operating System	Netbsd	Netbsd	1.4.2	All	alpha	All
Operating System	Netbsd	Netbsd	1.4.2	All	arm32	All
Operating System	Netbsd	Netbsd	1.4.2	All	sparc	All
Operating System	Netbsd	Netbsd	1.4.2	All	x86	All
Operating System	Netbsd	Netbsd	1.4.3	All	All	All

Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	sh3	All
Operating System	Netbsd	Netbsd	1.5	All	x86	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	beta	All	All
Operating System	Netbsd	Netbsd	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.4	All	alpha	All
Operating System	Netbsd	Netbsd	1.4	All	arm32	All
Operating System	Netbsd	Netbsd	1.4	All	sparc	All
Operating System	Netbsd	Netbsd	1.4	All	x86	All
Operating System	Netbsd	Netbsd	1.4.1	All	All	All
Operating System	Netbsd	Netbsd	1.4.1	All	alpha	All
Operating System	Netbsd	Netbsd	1.4.1	All	arm32	All
Operating System	Netbsd	Netbsd	1.4.1	All	sh3	All
Operating System	Netbsd	Netbsd	1.4.1	All	sparc	All
Operating System	Netbsd	Netbsd	1.4.1	All	x86	All
Operating System	Netbsd	Netbsd	1.4.2	All	All	All
Operating System	Netbsd	Netbsd	1.4.2	All	alpha	All
Operating System	Netbsd	Netbsd	1.4.2	All	arm32	All
Operating System	Netbsd	Netbsd	1.4.2	All	sparc	All
Operating System	Netbsd	Netbsd	1.4.2	All	x86	All

Operating System	Netbsd	Netbsd	1.4.3	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	sh3	All
Operating System	Netbsd	Netbsd	1.5	All	x86	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	beta	All	All
cpe:2.3:o:netbsd:netbsd:1.4:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4:*:alpha:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4:*:arm32:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4:*:sparc:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4:*:x86:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:alpha:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:arm32:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:sh3:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:sparc:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.1:*:x86:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.2:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.2:*:alpha:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.2:*:arm32:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.2:*:sparc:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.2:*:x86:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.4.3:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5:*:sh3:*:*:*:*:						

cpe:2.3:0:netbsd:netbsd:1.5:sh3:*****:
cpe:2.3:0:netbsd:netbsd:1.5:*:x86:*****:
cpe:2.3:0:netbsd:netbsd:1.5.1:*****:
cpe:2.3:0:netbsd:netbsd:1.5.2:*****:
cpe:2.3:0:netbsd:netbsd:1.5.3:*****:
cpe:2.3:0:netbsd:netbsd:1.6:beta:*****:
cpe:2.3:0:netbsd:netbsd:1.4:*****:
cpe:2.3:0:netbsd:netbsd:1.4:*:alpha:*****:
cpe:2.3:0:netbsd:netbsd:1.4:*:arm32:*****:
cpe:2.3:0:netbsd:netbsd:1.4:*:sparc:*****:
cpe:2.3:0:netbsd:netbsd:1.4:*:x86:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*:alpha:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*:arm32:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*:sh3:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*:sparc:*****:
cpe:2.3:0:netbsd:netbsd:1.4.1:*:x86:*****:
cpe:2.3:0:netbsd:netbsd:1.4.2:*****:
cpe:2.3:0:netbsd:netbsd:1.4.2:*:alpha:*****:
cpe:2.3:0:netbsd:netbsd:1.4.2:*:arm32:*****:
cpe:2.3:0:netbsd:netbsd:1.4.2:*:sparc:*****:
cpe:2.3:0:netbsd:netbsd:1.4.2:*:x86:*****:
cpe:2.3:0:netbsd:netbsd:1.4.3:*****:
cpe:2.3:0:netbsd:netbsd:1.5:*****:
cpe:2.3:0:netbsd:netbsd:1.5:*:sh3:*****:
cpe:2.3:0:netbsd:netbsd:1.5:*:x86:*****:
cpe:2.3:0:netbsd:netbsd:1.5.1:*****:
cpe:2.3:0:netbsd:netbsd:1.5.2:*****:
cpe:2.3:0:netbsd:netbsd:1.5.3:*****:

cpe:2.3:o:netbsd:netbsd:1.6:beta:*:*:*:*:

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](#)