

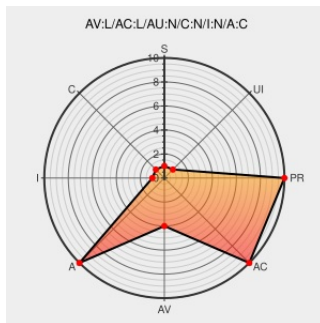


CVE-2006-3202

Published on: 06/23/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:58 PM UTC

CVE-2006-3202

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

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

The `ip6_savecontrol` function in NetBSD 2.0 through 3.0, under certain configurations, does not check to see if IPv4-mapped sockets are being used before processing IPv6 socket options, which allows local users to cause a denial of service (crash) by creating an IPv4-mapped IPv6 socket with the `SO_TIMESTAMP` socket option set, then sending an IPv4 packet through the socket.

CVE-2006-3202 has been assigned by [M](#) 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-ipv6-dos(27139)
SecurityTracker.com Archives - NetBSD Input Validation Error in Parsing IPv6 Socket Options Lets Local Users Deny Service	securitytracker.com text/html	SECTRAK 1016250
	ftp.netbsd.org text/plain	NETBSD NetBSD-SA2006-016

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

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	2.0.2	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	2.0.2	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:2.0.2:*****:.*						
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:2.0.2:*****:.*						
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 →](#)

© [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](#)