



CVE-2000-0489

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2000-0489
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	1999-09-05 04:00:00 UTC
Updated	2023-11-07 01:55:00 UTC
Description	FreeBSD, NetBSD, and OpenBSD allow an attacker to cause a denial of service by creating a large number of socket pairs

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	3.0	All	All	All
Operating System	Freebsd	Freebsd	3.1	All	All	All
Operating System	Freebsd	Freebsd	3.2	All	All	All
Operating System	Freebsd	Freebsd	3.3	All	All	All
Operating System	Freebsd	Freebsd	3.4	All	All	All
Operating System	Freebsd	Freebsd	3.5	All	All	All
Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	5.0	alpha	All	All
Operating System	Freebsd	Freebsd	3.0	All	All	All
Operating System	Freebsd	Freebsd	3.1	All	All	All
Operating System	Freebsd	Freebsd	3.2	All	All	All
Operating System	Freebsd	Freebsd	3.3	All	All	All
Operating System	Freebsd	Freebsd	3.4	All	All	All
Operating System	Freebsd	Freebsd	3.5	All	All	All
Operating System	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	5.0	alpha	All	All
Operating System	Netbsd	Netbsd	1.4	All	x86	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	sparc	All
Operating System	Netbsd	Netbsd	1.4.1	All	x86	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	All	x86	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	sparc	All
Operating System	Netbsd	Netbsd	1.4.1	All	x86	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	Openbsd	Openbsd	2.5	All	All	All
Operating System	Openbsd	Openbsd	2.6	All	All	All
Operating System	Openbsd	Openbsd	2.7	All	All	All
Operating System	Openbsd	Openbsd	2.5	All	All	All
Operating System	Openbsd	Openbsd	2.6	All	All	All
Operating System	Openbsd	Openbsd	2.7	All	All	All

References						
Reference	Source		Link		Tags	
IBM X-Force Exchange	XF		exchange.xforce.ibmcloud.com			
SecurityFocus			www.securityfocus.com			
SecurityFocus	BUGTRAQ		www.securityfocus.com			
BugTraq Archive: Local FreeBSD, Openbsd, NetBSD, DoS Vulnerability			www.securityfocus.com			
Multiple Vendor setsockopt() Denial of Service Vulnerability	BID		www.securityfocus.com			
BugTraq Archive: Local FreeBSD, Openbsd, NetBSD, DoS Vulnerability	BUGTRAQ		www.securityfocus.com			
CVE Program record	CVE.ORG		www.cve.org		canonical	
NVD vulnerability detail	NVD		nvd.nist.gov		canonical, analysis	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)