



CVE-2008-5736

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

Summary

CVE	CVE-2008-5736
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-26 18:30:00 UTC
Updated	2019-08-02 15:38:00 UTC
Description	Multiple unspecified vulnerabilities in FreeBSD 6 before 6.4-STABLE, 6.3 before 6.3-RELEASE-p7, 6.4 before 6.4-RELEAS

Risk And Classification

Problem Types: CWE-264 | NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	6.0	-	All	All
Operating System	Freebsd	Freebsd	6.3	-	All	All
Operating System	Freebsd	Freebsd	6.3	p1	All	All
Operating System	Freebsd	Freebsd	6.3	p2	All	All
Operating System	Freebsd	Freebsd	6.3	p3	All	All
Operating System	Freebsd	Freebsd	6.3	p4	All	All
Operating System	Freebsd	Freebsd	6.3	p5	All	All
Operating System	Freebsd	Freebsd	6.3	p6	All	All
Operating System	Freebsd	Freebsd	6.4	-	All	All
Operating System	Freebsd	Freebsd	7.0	-	All	All
Operating System	Freebsd	Freebsd	7.0	p1	All	All
Operating System	Freebsd	Freebsd	7.0	p3	All	All
Operating System	Freebsd	Freebsd	7.0	p4	All	All
Operating System	Freebsd	Freebsd	7.0	p5	All	All
Operating System	Freebsd	Freebsd	7.0	p6	All	All
Operating System	Freebsd	Freebsd	7.1	-	All	All
Operating System	Freebsd	Freebsd	7.1	rc1	All	All

Operating System	Freebsd	Freebsd	6.0	-	All	All
Operating System	Freebsd	Freebsd	6.3	-	All	All
Operating System	Freebsd	Freebsd	6.3	p1	All	All
Operating System	Freebsd	Freebsd	6.3	p2	All	All
Operating System	Freebsd	Freebsd	6.3	p3	All	All
Operating System	Freebsd	Freebsd	6.3	p4	All	All
Operating System	Freebsd	Freebsd	6.3	p5	All	All
Operating System	Freebsd	Freebsd	6.3	p6	All	All
Operating System	Freebsd	Freebsd	6.4	-	All	All
Operating System	Freebsd	Freebsd	7.0	-	All	All
Operating System	Freebsd	Freebsd	7.0	p1	All	All
Operating System	Freebsd	Freebsd	7.0	p3	All	All
Operating System	Freebsd	Freebsd	7.0	p4	All	All
Operating System	Freebsd	Freebsd	7.0	p5	All	All
Operating System	Freebsd	Freebsd	7.0	p6	All	All
Operating System	Freebsd	Freebsd	7.1	-	All	All
Operating System	Freebsd	Freebsd	7.1	rc1	All	All

References						
Reference			Source		ID	
IBM X-Force Exchange			XF		CVE-2017-15906	
FreeBSD netgraph and bluetooth Local Privilege Escalation Vulnerabilities			BID		75816	
FreeBSD <= 6.4 Netgraph Local Privledge Escalation Exploit			EXPLOIT-DB		45422	
FreeBSD 6x/7 protosw kernel Local Privledge Escalation Exploit			EXPLOIT-DB		45423	
50936			OSVDB		50936	
FreeBSD netgraph / bluetooth Sockets Privilege Escalation - Secunia Advisories - Vulnerability Intelligence - Secunia.com			SECUNIA		50936	
SecurityTracker: FreeBSD Netgraph and Bluetooth Protocol Stacks Let Local Users Gain Elevated Privileges			SECTRAK		50936	
FreeBSD-SA-08:13			FREEBSD		50936	
FreeBSD <= 6.4 Netgraph Local Privledge Escalation Exploit - SecurityReason.com			SREASON		50936	
CVE Program record			CVE.ORG		50936	
NVD vulnerability detail			NVD		50936	

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](#)