



CVE-2017-1087

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

Summary

CVE	CVE-2017-1087
State	PUBLIC
Assigner	secteam@freebsd.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-16 20:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In FreeBSD 10.x before 10.4-STABLE, 10.4-RELEASE-p3, and 10.3-RELEASE-p24 named paths are globally scoped, mea

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Freebsd	Freebsd	-	All	All	All
Operating System	Freebsd	Freebsd	-	All	All	All

References

Reference	Source
FreeBSD POSIX shm Globally Shared Namespace May Let Local Users Deny Service or Gain Elevated Privileges - SecurityTracker	SECTI
FreeBSD-SA-17:09	FREEI
FreeBSD CVE-2017-1087 Local Privilege Escalation Vulnerabiity	BID
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[43839](#) Juniper Junos Multiple Vulnerability (JSA11181,JSA11177,JSA11182,JSA11184,JSA11186)

© [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](#)