



CVE-2001-0402

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

Summary

CVE	CVE-2001-0402
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-06-18 04:00:00 UTC
Updated	2017-10-10 01:29:00 UTC
Description	IPFilter 3.4.16 and earlier does not include sufficient session information in its cache, which allows remote attackers to type

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Darren Reed	Ipfilter	All	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Openbsd	Openbsd	2.8	All	All	All
Operating System	Openbsd	Openbsd	2.8	All	All	All

References

Reference
Neohapsis Archives - FreeBSD Security - FreeBSD Security Advisory FreeBSD-SA-01:32.ipfilter - From security-advisories@FreeBSD.org
'A fragmentation attack against IP Filter' - MARC
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

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](#)