



CVE-2004-0218

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

Summary

CVE	CVE-2004-0218
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-05-04 04:00:00 UTC
Updated	2017-07-11 01:29:00 UTC
Description	isakmpd in OpenBSD 3.4 and earlier allows remote attackers to cause a denial of service (infinite loop) via an ISAKMP pac

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Openbsd	Openbsd	All	All	All	All

References

Reference	Source	Link
'R7-0018: OpenBSD isakmpd payload handling denial-of-service vulnerabilities' - MARC	BUGTRAQ	marc.info
Secunia - Advisories - OpenBSD isakmpd Payload Handling Denial of Service Vulnerabilities	SECUNIA	secunia.com
SecurityTracker.com Archives - isakmpd Payload Handling Flaw Lets Remote Users Crash the Daemon	SECTrack	www.securitytracker.com
US-CERT Vulnerability Note VU#349113	CERT-VN	www.kb.cert.org
404 Page Not Found	MISC	www.rapid7.com
OpenBSD ISAKMPD Zero Payload Length Denial Of Service Vulnerability	BID	www.securityfocus.com
OpenBSD 4.0 errata	OPENBSD	www.openbsd.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)