



CVE-2005-0960

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

Summary

CVE	CVE-2005-0960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2008-09-05 20:47:00 UTC
Description	Multiple vulnerabilities in the SACK functionality in (1) tcp_input.c and (2) tcp_usreq.c OpenBSD 3.5 and 3.6 allow remote users to cause a denial of service (DoS) by sending a large number of SYN packets to the target system. The vulnerability is due to a buffer overflow in the SACK functionality. The vulnerability is present in OpenBSD 3.5 and 3.6. The vulnerability is caused by a buffer overflow in the SACK functionality. The vulnerability is present in OpenBSD 3.5 and 3.6. The vulnerability is caused by a buffer overflow in the SACK functionality.

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	3.5	All	All	All
Operating System	Openbsd	Openbsd	3.6	All	All	All
Operating System	Openbsd	Openbsd	3.5	All	All	All
Operating System	Openbsd	Openbsd	3.6	All	All	All

References

Reference	Source	Link
OpenBSD TCP Stack Remote Denial Of Service Vulnerability	BID	www.securityfocus.com/bid/10441
SecurityTracker.com Archives - OpenBSD tcp(4) Bugs in Processing SACK Options Let Remote Users Deny Service	SECTrack	securitytracker.com/showDetails.cfm?id=10441
OpenBSD 3.5 errata	OPENBSD	www.openbsd.org/errata35.html
OpenBSD 3.8 errata	OPENBSD	www.openbsd.org/errata38.html
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve-2005-0960
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2005-0960

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](#)