



CVE-2008-3234

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

Summary

CVE	CVE-2008-3234
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-18 16:41:00 UTC
Updated	2017-09-29 01:31:00 UTC
Description	sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to ol

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Debian	Debian Linux	All	All	All	All
Application	Openbsd	Openssh	4.0	All	All	All
Application	Openbsd	Openssh	4.0	All	All	All

References

Reference	Source	Link	Tags
Debian OpenSSH Remote SELinux Privilege Elevation Exploit (auth)	EXPLOIT-DB	www.exploit-db.com	
Debian OpenSSH SELinux Privilege Escalation Vulnerability	BID	www.securityfocus.com	Exploit
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-07-21	Joshua Bressers	Upon investigating this issue, the Red Hat Security Response Team has determined that thi

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](#)