



CVE-2008-5157

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

Summary

CVE	CVE-2008-5157
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-18 16:00:00 UTC
Updated	2017-08-08 01:33:00 UTC
Description	tau 2.16.4 allows local users to overwrite arbitrary files via a symlink attack on a (1) /tmp/makefile.tau.*##### or (2) /tmp/m

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uoregon	Tau	2.16.4	All	All	All
Application	Uoregon	Tau	2.16.4	All	All	All

References

Reference	Source	Link
#506348 - CVE-2008-5157: allows local users to overwrite arbitrary files via a symlink attack - Debian Bug report logs	MISC	bugs.de
Re: Possible mass bug filing: The possibility of attack with the help of symlinks in some Debian packages	MLIST	lists.deb
TAU Tuning and Analysis Utilities Insecure Temporary File Creation Vulnerabilities	BID	www.se
uvw.ru/report.sid.txt	MISC	uvw.ru
IBM X-Force Exchange	XF	exchang
TAU Insecure Temporary Files - Secunia.com	SECUNIA	secunia.
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

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](#)