



CVE-2008-4955

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

Summary

CVE	CVE-2008-4955
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-05 15:00:00 UTC
Updated	2009-07-20 04:00:00 UTC
Description	freevo.real in freevo 1.8.1 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/*-#####.pid, (2) /tmp

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Duncan Webb	Freevo	1.8.1	All	All	All
Application	Duncan Webb	Freevo	1.8.1	All	All	All

References

Reference	Source	Link
#496373 - The possibility of attack with the help of symlinks in some Debian packages - Debian Bug report logs	MISC	bugs.debian.o
235770 – (debian-tempfile) [Tracker] Tempfile issues found in Debian	MISC	bugs.gentoo.o
oss-security - CVE requests: tempfile issues for aview, mgetty, openoffice, crossfire	MLIST	www.openwall
404 Not Found	MISC	dev.gentoo.org
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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)