



CVE-2008-5703

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

Summary

CVE	CVE-2008-5703
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-22 15:30:00 UTC
Updated	2009-08-19 05:22:00 UTC
Description	gpsdrive (aka gpsdrive-scripts) 2.10~pre4 allows local users to overwrite arbitrary files via a symlink attack on the (a) /tmp/.

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gpsdrive	Gpsdrive	1.32	All	All	All
Application	Gpsdrive	Gpsdrive	1.33	All	All	All
Application	Gpsdrive	Gpsdrive	2.09	All	All	All
Application	Gpsdrive	Gpsdrive	1.32	All	All	All
Application	Gpsdrive	Gpsdrive	1.33	All	All	All
Application	Gpsdrive	Gpsdrive	2.09	All	All	All
Application	Gpsdrive	Gpsdrive	All	pre2	All	All

References

Reference	Source	Link
oss-security - CVE id request: gpsdrive	MLIST	openwall.com
GpsDrive "geo-code" Insecure Temporary Files - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 9 Update: gpsdrive-2.09-7.fc9	FEDORA	www.redhat.co
Fedora update for gpsdrive - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
GpsDrive Multiple Insecure Temporary File Creation Vulnerabilities	BID	www.securityfo
GpsDrive / Bugs / #5 signalposreq(): use mkstemp	CONFIRM	sourceforge.ne
#508597 - gpsdriver: allows local users to overwrite arbitrary files via a symlink attack - Debian Bug report logs	CONFIRM	bugs.debian.or

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