



CVE-2007-0752

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

Summary

CVE	CVE-2007-0752
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-24 22:30:00 UTC
Updated	2017-07-29 01:30:00 UTC
Description	The PPP daemon (pppd) in Apple Mac OS X 10.4.8 checks ownership of the stdin file descriptor to determine if the invoker

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.4.8	All	All	All
Operating System	Apple	Mac Os X	10.4.8	All	All	All
Operating System	Apple	Mac Os X Server	10.4.8	All	All	All
Operating System	Apple	Mac Os X Server	10.4.8	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xfc
SecurityTracker.com Archives - Mac OS X pppd Plugin Loading Feature Lets Local Users Gain Root Privileges	SECTrack	www.security
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.c
APPLE-SA-2007-05-24 Security Update 2007-005	APPLE	lists.apple.co
Apple Mac OS X Security Update for Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com
20070524 Apple Computer Mac OS X pppd Plugin Loading Privilege Escalation Vulnerability	IDEFENSE	labs.idefense
Apple Mac OS X 2007-005 Multiple Security Vulnerabilities	BID	www.security
35144	OSVDB	www.osvdb.c
About Security Update 2007-005	CONFIRM	docs.info.app
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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