



# CVE-2010-4706

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

## Summary

<b>CVE</b>	CVE-2010-4706
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-01-24 19:00:00 UTC
<b>Updated</b>	2023-11-07 02:06:00 UTC
<b>Description</b>	The pam_sm_close_session function in pam_xauth.c in the pam_xauth module in Linux-PAM (aka pam) 1.1.2 and earlier d

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.1.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.10.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.2.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.2.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.3.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.4.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.5.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.2	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.3	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.7.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.7.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.8.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.8.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.9.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.0	All	All	All

Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.2	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.3	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.4	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.1.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.1.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.1.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.10.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.2.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.2.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.3.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.4.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.5.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.2	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.6.3	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.7.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.7.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.8.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.8.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	0.99.9.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.2	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.3	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.0.4	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.1.0	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	1.1.1	All	All	All
Application	<a href="#">Linux-pam</a>	<a href="#">Linux-pam</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Gentoo Linux Documentation -- Linux-PAM: Multiple vulnerabilities	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
git.altlinux.org - pam.git/commit	CONFIRM	<a href="https://git.altlinux.org">git.altlinux.org</a>	Patch

Linux-PAM 'pam_xauth' Module Denial of Service and Security Bypass Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
oss-security - Re: Minor security flaw with pam_xauth	MLIST	<a href="http://openwall.com">openwall.com</a>	Patch
git.altlinux.org - pam.git/commit		<a href="http://git.altlinux.org">git.altlinux.org</a>	
Security Advisory SA49711 - Gentoo update for pam - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)