

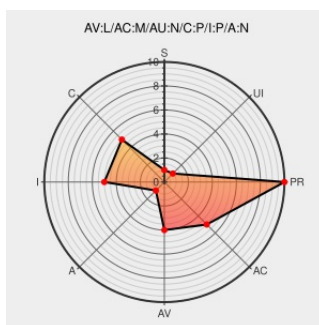


CVE-2010-3316

Published on: 01/24/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:23:00 AM UTC

CVE-2010-3316

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux-pam](#) from [Linux-pam](#) contain the following vulnerability:

The `run_coprocess` function in `pam_xauth.c` in the `pam_xauth` module in Linux-PAM (aka pam) before 1.1.2 does not check the return values of the `setuid`, `setgid`, and `setgroups` system calls, which might allow local users to read arbitrary files by executing a program that relies on the `pam_xauth` PAM check.

CVE-2010-3316 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access Vector

LOCAL

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Pluggable Auth Modules / Bugs / #314 Minor security flaw with pam_xauth

[sourceforge.net](#)
[text/html](#)

[MISC sourceforge.net/tracker/?func=detail&aid=3028213&group_id=6663&atid=106663](#)

Gentoo Linux Documentation -- Linux-PAM: Multiple vulnerabilities

[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-201206-31](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2011-0606](#)

git.altlinux.org - pam.git/commit

[Patch](#)
[web.archive.org](#)
[text/xml](#)

[MISC git.altlinux.org/people/ldv/packages/?p=pam.git%3Ba=commit%3Bh=06f882f30092a39a1db867c9744b2ca8d60e4ad6](#)

Support / Security / Advisories / / MDVSA-2010:220 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2010:220
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2010:0819
oss-security - Re: Minor security flaw with pam_xauth	Patch openwall.com text/html	 MLIST [oss-security] 20100928 Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth	Patch www.openwall.com text/html	 MLIST [oss-security] 20100924 Re: Minor security flaw with pam_xauth
oss-security - Minor security flaw with pam_xauth	openwall.com text/html	 MLIST [oss-security] 20100816 Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth	Patch openwall.com text/html	 MLIST [oss-security] 20100921 Re: Minor security flaw with pam_xauth
[Security-announce] VMSA-2011-0004 VMware ESX/ESXi SLPD denial of service vulnerability and ESX third party updates for Service Console packages bind, pam, and rpm	lists.vmware.com text/html	 MLIST [security-announce] 20110307 VMSA-2011-0004 VMware ESX/ESXi SLPD denial of service vulnerability and ESX third party updates for Service Console packages bind, pam, and rpm
rhnl.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2010:0891
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20110308 VMSA-2011-0004 VMware ESX/ESXi SLPD denial of service vulnerability and ESX third party updates for Service Console packages bind, pam, and rpm.
VMSA-2011-0004	www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2011-0004.html
Security Advisory SA49711 - Gentoo update for pam - Secunia	web.archive.org text/html	 SECUNIA 49711
637898 – (CVE-2010-3316) CVE-2010-3316 pam: pam_xauth missing return value checks from setuid() and similar calls	Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=637898
oss-security - Re: Minor security flaw with pam_xauth	Patch openwall.com text/html	 MLIST [oss-security] 20100921 Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth	Patch openwall.com text/html	 MLIST [oss-security] 20100927 Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth	Patch openwall.com text/html	 MLIST [oss-security] 20101025 Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth	openwall.com text/html	 MLIST [oss-security] 20100928 Re: Minor security flaw with pam_xauth

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-pam	Linux-pam	0.99.1.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.10.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.2.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.2.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.3.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.4.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.5.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.2	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.3	All	All	All
Application	Linux-pam	Linux-pam	0.99.7.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.7.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.8.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.8.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.9.0	All	All	All
Application	Linux-pam	Linux-pam	1.0.0	All	All	All
Application	Linux-pam	Linux-pam	1.0.1	All	All	All
Application	Linux-pam	Linux-pam	1.0.2	All	All	All
Application	Linux-pam	Linux-pam	1.0.3	All	All	All
Application	Linux-pam	Linux-pam	1.0.4	All	All	All
Application	Linux-pam	Linux-pam	1.1.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.1.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.10.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.2.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.2.1	All	All	All

Application	Linux-pam	Linux-pam	0.99.3.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.4.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.5.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.2	All	All	All
Application	Linux-pam	Linux-pam	0.99.6.3	All	All	All
Application	Linux-pam	Linux-pam	0.99.7.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.7.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.8.0	All	All	All
Application	Linux-pam	Linux-pam	0.99.8.1	All	All	All
Application	Linux-pam	Linux-pam	0.99.9.0	All	All	All
Application	Linux-pam	Linux-pam	1.0.0	All	All	All
Application	Linux-pam	Linux-pam	1.0.1	All	All	All
Application	Linux-pam	Linux-pam	1.0.2	All	All	All
Application	Linux-pam	Linux-pam	1.0.3	All	All	All
Application	Linux-pam	Linux-pam	1.0.4	All	All	All
Application	Linux-pam	Linux-pam	1.1.0	All	All	All
Application	Linux-pam	Linux-pam	All	All	All	All
cpe:2.3:a:linux-pam:linux-pam:0.99.1.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.10.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.2.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.2.1:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.3.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.4.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.5.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.6.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.6.1:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.6.2:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.6.3:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.7.0:*****:						
cpe:2.3:a:linux-pam:linux-pam:0.99.7.1:*****:						

cpe:2.3:a:linux-pam:linux-pam:0.99.8.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.8.1:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.9.0:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.0:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.1:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.2:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.3:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.4:*****:
cpe:2.3:a:linux-pam:linux-pam:1.1.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.1.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.10.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.2.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.2.1:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.3.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.4.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.5.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.6.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.6.1:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.6.2:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.6.3:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.7.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.7.1:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.8.0:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.8.1:*****:
cpe:2.3:a:linux-pam:linux-pam:0.99.9.0:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.0:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.1:*****:
cpe:2.3:a:linux-pam:linux-pam:1.0.2:*****:

cpe:2.3:a:linux-pam:linux-pam:1.0.3:~::~::~:
cpe:2.3:a:linux-pam:linux-pam:1.0.4:~::~::~:
cpe:2.3:a:linux-pam:linux-pam:1.1.0:~::~::~:
cpe:2.3:a:linux-pam:linux-pam:~::~::~:

No vendor comments have been submitted for this CVE

← Previous IDNext ID→

© [CVE.report](#) 2023  |

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](#)