CVE-2010-3435

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-3435
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-24 18:00:00 UTC
Updated	2023-02-13 04:24:00 UTC
Description	The (1) pam_env and (2) pam_mail modules in Linux-PAM (aka pam) before 1.1.2 use root privileges during read access to

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Gentoo Linux Documentation -- Linux-PAM: Multiple vulnerabilities
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
641335 – (CVE-2010-3435) CVE-2010-3435 pam: pam_env and pam_mail accessing users' file with root privileges
git.altlinux.org - pam.git/commit

Support / Security / Advisories / / MDVSA-2010:220 | Mandriva
rhn.redhat.com | Red Hat Support
oss-security - Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth
oss-security - 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 Consc
rhn.redhat.com | Red Hat Support
SecurityFocus
VMSA-2011-0004
Security Advisory SA49711 - Gentoo update for pam - Secunia
oss-security - Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth
git.altlinux.org - pam.git/commit
oss-security - Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth
oss-security - Re: Minor security flaw with pam_xauth
CVE Program record
NVD vulnerability detail

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 registred 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