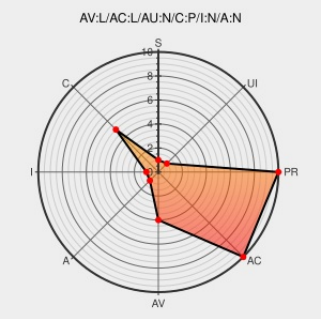
CVE-2005-2977

Published on: 10/31/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-2977

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pam from Pam contain the following vulnerability:

The SELinux version of PAM before 0.78 r3 allows local users to perform brute force password guessing attacks via unix_chkpwd, which does not log failed guesses or delay its responses.

CVE-2005-2977 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
168181 – CVE-2005-2977 unix_chkpwd helper doesn't verify requesting user if SELinux is enabled	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/bugzilla/show_bug.cgi?id=168181
No Description Provided	cvs.sourceforge.net Inactive Link Not Archived	CONFIRM cvs.sourceforge.net/viewcvs.py/pam/Linux-PAM/NEWS?rev=1.6&view=markup
PAM Unix_Chkpwd Unauthorized Access Vulnerability	cve.report (archive) text/html	BID 15217
Gentoo Linux Documentation -- SELinux PAM: Local password guessing attack	Patch Vendor Advisory www.gentoo.org text/html	GENTOO GLSA-200510-22
Secunia - Advisories - Gentoo update for pam	Patch	SECUNIA 17365

	Vendor Advisory web.archive.org text/html	
Secunia - Advisories - SELinux "unix_chkpwd" Security Bypass Security Issue	web.archive.org text/html	SECUNIA 17352
Secunia - Advisories - Fedora update for pam	web.archive.org text/html	SECUNIA 17346
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2005-2227
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:805
Secunia - Advisories - Red Hat update for pam	web.archive.org text/html	SECUNIA 17350
SecurityTracker.com Archives - PAM with SELinux Lets Local Users Invoke unix_chkpwd to Conduct Password Guessing Attacks	securitytracker.com text/html	SECTRACK 1015111
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10193

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pam	Pam	All	All	selinux	All

cpe:2.3:a:pam:pam:*:*:selinux:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→