CVE-2005-2641

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2005-2641
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-08-23 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Unknown vulnerability in pam_ldap before 180 does not properly handle a new password policy control, which could allow a

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Padl Software	Pam Ldap	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Advisories - Mandriva	af854a3a-2127-422b-91ae-364
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364
Secunia - Advisories - Mandriva update for nss_ldap/pam_ldap	af854a3a-2127-422b-91ae-364
SecurityFocus	af854a3a-2127-422b-91ae-364
Secunia - Advisories - Red Hat update for openldap / nss_ldap	af854a3a-2127-422b-91ae-364
rawhide report: 20050818 changes	af854a3a-2127-422b-91ae-364
US-CERT Vulnerability Note VU#778916	af854a3a-2127-422b-91ae-364
[#RPL-680] pam_ldap module in nss_ldap handles locked accounts incorrectly CVE-2006-5170 - rPath JIRA	af854a3a-2127-422b-91ae-364
PADL Software PAM_LDAP Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364
Repository / Oval Repository	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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