



# CVE-2006-5170

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

## Summary

<b>CVE</b>	CVE-2006-5170
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-10-10 04:06:00 UTC
<b>Updated</b>	2022-02-25 19:20:00 UTC
<b>Description</b>	pam_ldap in nss_ldap on Red Hat Enterprise Linux 4, Fedora Core 3 and earlier, and possibly other distributions does not r

## Risk And Classification

**Problem Types:** CWE-755

## NVD Known Affected Configurations (CPE 2.3)


Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora Core</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	linux_kernel_2.6.9	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	4.0	All	linux_kernel_2.6.9	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	4.0_s390	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	4.0_s390x	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Big Endian</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	All	All	All	All

## References

### Reference

[Debian -- Security Information -- DSA-1203-1 libpam-ldap](#)

[nss\\_ldap Error in pam\\_ldap in Processing PasswordPolicyReponse Messages May Let Remote Users Bypass Authentication - SecurityTracke](#)

Security Announcement
SUSE Update for Multiple Packages - Advisories - Secunia
Advisories - Mandriva Linux
pam_ldap "PasswordPolicyResponse" Security Bypass - Secunia.com
Red Hat update for nss_ldap - Advisories - Secunia
PADL Software Pam_Ldap PasswordPolicyResponse Authentication Bypass Vulnerability
Debian update for pam_ldap - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
207286 – CVE-2006-5170 When using LDAP for authentication, xscreensaver allows access if account locked out.
Mandriva update for pam_ldap - Secunia.com
pam_ldap: Authentication bypass vulnerability — Gentoo Linux Documentation
2006-0061
[#RPL-680] pam_ldap module in nss_ldap handles locked accounts incorrectly CVE-2006-5170 - rPath JIRA
Trustix Update for Multiple Packages - Advisories - Secunia
bugzilla.padl.com/show_bug.cgi
Repository / Oval Repository
rhn.redhat.com   Red Hat Support
Gentoo update for pam_ldap - Advisories - Secunia
SecurityFocus
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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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