



CVE-2009-1073

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

Summary

CVE	CVE-2009-1073
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-31 18:24:00 UTC
Updated	2009-04-08 05:36:00 UTC
Description	nss-ldapd before 0.6.8 uses world-readable permissions for the /etc/nss-ldapd.conf file, which allows local users to obtain a

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Debian	Nss-ldapd	0.1	All	All	All
Application	Debian	Nss-ldapd	0.2	All	All	All
Application	Debian	Nss-ldapd	0.2.1	All	All	All
Application	Debian	Nss-ldapd	0.3	All	All	All
Application	Debian	Nss-ldapd	0.4	All	All	All
Application	Debian	Nss-ldapd	0.4.1	All	All	All
Application	Debian	Nss-ldapd	0.5	All	All	All
Application	Debian	Nss-ldapd	0.6	All	All	All
Application	Debian	Nss-ldapd	0.6.1	All	All	All
Application	Debian	Nss-ldapd	0.6.2	All	All	All
Application	Debian	Nss-ldapd	0.6.3	All	All	All
Application	Debian	Nss-ldapd	0.6.4	All	All	All
Application	Debian	Nss-ldapd	0.6.5	All	All	All
Application	Debian	Nss-ldapd	0.6.6	All	All	All
Application	Debian	Nss-ldapd	All	All	All	All
Application	Debian	Nss-ldapd	0.1	All	All	All
Application	Debian	Nss-ldapd	0.2	All	All	All

Application	Debian	Nss-Ildap	0.2.1	All	All	All
Application	Debian	Nss-Ildap	0.3	All	All	All
Application	Debian	Nss-Ildap	0.4	All	All	All
Application	Debian	Nss-Ildap	0.4.1	All	All	All
Application	Debian	Nss-Ildap	0.5	All	All	All
Application	Debian	Nss-Ildap	0.6	All	All	All
Application	Debian	Nss-Ildap	0.6.1	All	All	All
Application	Debian	Nss-Ildap	0.6.2	All	All	All
Application	Debian	Nss-Ildap	0.6.3	All	All	All
Application	Debian	Nss-Ildap	0.6.4	All	All	All
Application	Debian	Nss-Ildap	0.6.5	All	All	All
Application	Debian	Nss-Ildap	0.6.6	All	All	All

References			
Reference	Source	Link	
oss-security - Re: CVE request -- ucd-snmp / net-snmp, libnss-ldapd / nss_ldap	MLIST	www.openwa	
oss-security - Re: CVE request -- ucd-snmp / net-snmp, libnss-ldapd / nss_ldap	MLIST	www.openwa	
PADL nss_ldap '/etc/nss_ldapd.conf' Local Information Disclosure Vulnerability	BID	www.security	
Debian update for nss-ldapd - Secunia.com	SECUNIA	secunia.com	
Debian -- Security Information -- DSA-1758-1 nss-ldapd	DEBIAN	www.debian.o	
arthurenhella.demon.nl/viewvc/nss-ldapd/nss-ldapd/man/nss-ldapd.conf.5.xml	CONFIRM	arthurenhella	
CVE-2009-1073	MISC	launchpad.ne	
oss-security - Re: CVE request -- ucd-snmp / net-snmp, libnss-ldapd / nss_ldap	MLIST	www.openwa	
oss-security - CVE request -- ucd-snmp / net-snmp, libnss-ldapd / nss_ldap	MLIST	www.openwa	
nss-ldapd: news	CONFIRM	ch.tudelft.nl	
#520476 - libnss-ldapd: /etc/nss-ldapd.conf is created world-readable, exposing bindpw - Debian Bug report logs	CONFIRM	bugs.debian.o	
arthurenhella.demon.nl/viewvc/nss-ldapd/nss-ldapd/debian/libnss-ldapd.postinst	CONFIRM	arthurenhella	
CVE Program record	CVE.ORG	www.cve.org	
NVD vulnerability detail	NVD	nvd.nist.gov	

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report