



CVE-2011-1025

Published on: 03/19/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:08 AM UTC

CVE-2011-1025

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openldap](#) from [Openldap](#) contain the following vulnerability:

bind.cpp in back-ndb in OpenLDAP 2.4.x before 2.4.24 does not require authentication for the root Distinguished Name (DN), which allows remote attackers to bypass intended access restrictions via an arbitrary password.

CVE-2011-1025 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

USN-1100-1: OpenLDAP vulnerabilities | Ubuntu

www.ubuntu.com
text/html

[UBUNTU USN-1100-1](#)

[Patch](#)
www.openldap.org
text/x-diff

[CONFIRM](#)
www.openldap.org/devel/cvsweb.cgi/servers/slapd/back-ndb/bind.cpp.diff?r1=1.5&r2=1.8

OpenLDAP 2.4.24 available

www.openldap.org
text/html

[MLIST \[openldap-announce\] 20110212 OpenLDAP 2.4.24 available](#)

Support

www.redhat.com
text/html

[REDHAT RHSA-2011:0347](#)

Support / Security / Advisories // MDVSA-2011:056 | Mandriva

www.mandriva.com
text/html

[MANDRIVA MDVSA-2011:056](#)

OpenLDAP Multiple Vulnerabilities - Secunia.com

[Vendor Advisory](#)

[SECUNIA 43331](#)

	web.archive.org text/html	
Red Hat update for openldap - Secunia.com	web.archive.org text/html	 SECUNIA 43718
Gentoo Linux Documentation -- OpenLDAP: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-201406-36
OpenLDAP back-ndb Lets Remote Users Authenticate Without a Valid Password - SecurityTracker	securitytracker.com text/html	 SECTRACK 1025190
OpenLDAP ITS - Software Bugs/6661	www.openldap.org text/html	 CONFIRM www.openldap.org/its/index.cgi/Software%20Bugs?id=6661
680472 – (CVE-2011-1025) CVE-2011-1025 openldap: rootpw not verified via slapd.conf when using the NDB backend	Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=680472
oss-security - Re: CVE Request -- OpenLDAP -- two issues	openwall.com text/html	 MLIST [oss-security] 20110225 Re: CVE Request -- OpenLDAP -- two issue
Webmail - OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2011-0665
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	kb.juniper.net text/html	 CONFIRM kb.juniper.net/InfoCenter/index?page=content&id=JSA10705
oss-security - CVE Request -- OpenLDAP -- two issues	openwall.com text/html	 MLIST [oss-security] 20110224 CVE Request -- OpenLDAP -- two issues

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openldap	Openldap	2.4.10	All	All	All
Application	Openldap	Openldap	2.4.11	All	All	All
Application	Openldap	Openldap	2.4.12	All	All	All
Application	Openldap	Openldap	2.4.13	All	All	All
Application	Openldap	Openldap	2.4.14	All	All	All
Application	Openldap	Openldap	2.4.15	All	All	All
Application	Openldap	Openldap	2.4.16	All	All	All
Application	Openldap	Openldap	2.4.17	All	All	All
Application	Openldap	Openldap	2.4.18	All	All	All
Application	Openldap	Openldap	2.4.19	All	All	All
Application	Openldap	Openldap	2.4.20	All	All	All

Application	Openldap	Openldap	2.4.21	All	All	All
Application	Openldap	Openldap	2.4.22	All	All	All
Application	Openldap	Openldap	2.4.23	All	All	All
Application	Openldap	Openldap	2.4.6	All	All	All
Application	Openldap	Openldap	2.4.7	All	All	All
Application	Openldap	Openldap	2.4.8	All	All	All
Application	Openldap	Openldap	2.4.9	All	All	All
Application	Openldap	Openldap	2.4.10	All	All	All
Application	Openldap	Openldap	2.4.11	All	All	All
Application	Openldap	Openldap	2.4.12	All	All	All
Application	Openldap	Openldap	2.4.13	All	All	All
Application	Openldap	Openldap	2.4.14	All	All	All
Application	Openldap	Openldap	2.4.15	All	All	All
Application	Openldap	Openldap	2.4.16	All	All	All
Application	Openldap	Openldap	2.4.17	All	All	All
Application	Openldap	Openldap	2.4.18	All	All	All
Application	Openldap	Openldap	2.4.19	All	All	All
Application	Openldap	Openldap	2.4.20	All	All	All
Application	Openldap	Openldap	2.4.21	All	All	All
Application	Openldap	Openldap	2.4.22	All	All	All
Application	Openldap	Openldap	2.4.23	All	All	All
Application	Openldap	Openldap	2.4.6	All	All	All
Application	Openldap	Openldap	2.4.7	All	All	All
Application	Openldap	Openldap	2.4.8	All	All	All
Application	Openldap	Openldap	2.4.9	All	All	All
cpe:2.3:a:openldap:openldap:2.4.10:*****:						
cpe:2.3:a:openldap:openldap:2.4.11:*****:						
cpe:2.3:a:openldap:openldap:2.4.12:*****:						
cpe:2.3:a:openldap:openldap:2.4.13:*****:						
cpe:2.3:a:openldap:openldap:2.4.14:*****:						
cpe:2.3:a:openldap:openldap:2.4.15:*****:						
cpe:2.3:a:openldap:openldap:2.4.16:*****:						
cpe:2.3:a:openldap:openldap:2.4.17:*****:						

cpe:2.3:a:openldap:openldap:2.4.18:*****:
cpe:2.3:a:openldap:openldap:2.4.19:*****:
cpe:2.3:a:openldap:openldap:2.4.20:*****:
cpe:2.3:a:openldap:openldap:2.4.21:*****:
cpe:2.3:a:openldap:openldap:2.4.22:*****:
cpe:2.3:a:openldap:openldap:2.4.23:*****:
cpe:2.3:a:openldap:openldap:2.4.6:*****:
cpe:2.3:a:openldap:openldap:2.4.7:*****:
cpe:2.3:a:openldap:openldap:2.4.8:*****:
cpe:2.3:a:openldap:openldap:2.4.9:*****:
cpe:2.3:a:openldap:openldap:2.4.10:*****:
cpe:2.3:a:openldap:openldap:2.4.11:*****:
cpe:2.3:a:openldap:openldap:2.4.12:*****:
cpe:2.3:a:openldap:openldap:2.4.13:*****:
cpe:2.3:a:openldap:openldap:2.4.14:*****:
cpe:2.3:a:openldap:openldap:2.4.15:*****:
cpe:2.3:a:openldap:openldap:2.4.16:*****:
cpe:2.3:a:openldap:openldap:2.4.17:*****:
cpe:2.3:a:openldap:openldap:2.4.18:*****:
cpe:2.3:a:openldap:openldap:2.4.19:*****:
cpe:2.3:a:openldap:openldap:2.4.20:*****:
cpe:2.3:a:openldap:openldap:2.4.21:*****:
cpe:2.3:a:openldap:openldap:2.4.22:*****:
cpe:2.3:a:openldap:openldap:2.4.23:*****:
cpe:2.3:a:openldap:openldap:2.4.6:*****:
cpe:2.3:a:openldap:openldap:2.4.7:*****:
cpe:2.3:a:openldap:openldap:2.4.8:*****:
cpe:2.3:a:openldap:openldap:2.4.9:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)