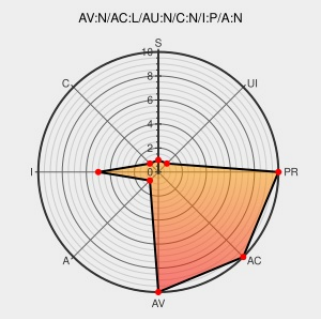
CVE-2006-2754

Published on: 06/01/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-2754

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



Certain versions of Openldap from Openldap contain the following vulnerability:

Stack-based buffer overflow in st.c in slurpd for OpenLDAP before 2.3.22 might allow attackers to execute arbitrary code via a long hostname.

CVE-2006-2754 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Mandriva update for openldap - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 20495
Secunia - Advisories - Ubuntu update for OpenLDAP	web.archive.org text/html	SECUNIA 20848
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 25659
servers/slurpd/st.c - diff - 1.22	Patch www.openldap.org text/html	CONFIRM www.openldap.org/devel/cvsweb.cgi/servers/slurpd/st.c.diff?r1=1.21&r2=1.22&hideattic=1&sortbydate=0&f=h
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060609 rPSA-2006-0099-1 openldap openldap-clients openldap-servers

OpenLDAP slurpd Status File Handling Buffer Overflow - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 20126
OpenPKG Corporation: Security: Security Advisories	Patch www.openpkg.org text/html	OPENPKG OpenPKG-SA-2006.008
USN-305-1: OpenLDAP vulnerability | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-305-1
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:096
OpenLDAP, 2.4.33 Release Changes	Patch www.openldap.org text/html	CONFIRM www.openldap.org/software/release/changes.html
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-1921
CVS log for servers/slurpd/Attic/st.c	Patch www.openldap.org text/html	CONFIRM www.openldap.org/devel/cvsweb.cgi/servers/slurpd/st.c?hideattic=1&sortbydate=0#rev1.22
Secunia - Advisories - Gentoo update for openldap	web.archive.org text/html	SECUNIA 20685
Gentoo Linux Documentation -- OpenLDAP: Buffer overflow	www.gentoo.org text/html	GENTOO GLSA-200606-17

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	2.2.1	All	All	All
Application	Openldap	Openldap	2.2.11	All	All	All
Application	Openldap	Openldap	2.2.12	All	All	All
Application	Openldap	Openldap	2.2.13	All	All	All
Application	Openldap	Openldap	2.2.14	All	All	All
Application	Openldap	Openldap	2.2.15	All	All	All
Application	Openldap	Openldap	2.2.16	All	All	All
Application	Openldap	Openldap	2.2.17	All	All	All
Application	Openldap	Openldap	2.2.18	All	All	All
Application	Openldap	Openldap	2.2.19	All	All	All
Application	Openldap	Openldap	2.2.20	All	All	All

Application	Openldap	Openldap	2.2.21	All	All	All
Application	Openldap	Openldap	2.2.1	All	All	All
Application	Openldap	Openldap	2.2.11	All	All	All
Application	Openldap	Openldap	2.2.12	All	All	All
Application	Openldap	Openldap	2.2.13	All	All	All
Application	Openldap	Openldap	2.2.14	All	All	All
Application	Openldap	Openldap	2.2.15	All	All	All
Application	Openldap	Openldap	2.2.16	All	All	All
Application	Openldap	Openldap	2.2.17	All	All	All
Application	Openldap	Openldap	2.2.18	All	All	All
Application	Openldap	Openldap	2.2.19	All	All	All
Application	Openldap	Openldap	2.2.20	All	All	All
Application	Openldap	Openldap	2.2.21	All	All	All

cpe:2.3:a:openldap:openldap:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.16:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.17:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.18:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.19:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.20:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.21:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.14:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.15:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.16:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.17:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.18:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.19:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.20:*:*:*:*:*:*:*:

cpe:2.3:a:openldap:openldap:2.2.21:*:*:*:*:*:*:*:

← 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 registred 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