



CVE-2002-2043

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

Summary

CVE	CVE-2002-2043
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2008-09-05 20:32:00 UTC
Description	SQL injection vulnerability in the LDAP and MySQL authentication patch for Cyrus SASL 1.5.24 and 1.5.27 allows remote a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyrus	Sasl	1.5.24	All	All	All
Application	Cyrus	Sasl	1.5.27	All	All	All
Application	Cyrus	Sasl	1.5.24	All	All	All
Application	Cyrus	Sasl	1.5.27	All	All	All

References

Reference	Source
20020402 SASL (v1/v2) MYSQL/LDAP authentication patch.	BUGTRAQ
ISS X-Force Database: cyrus-sasl-patch-pop-access (8748): Cyrus SASL LDAP+MySQL patch allows user unauthorized POP access	XF
4409	BID
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2006-08-30	Mark J Cox	Not vulnerable. This issue only affects a third-party patch to Cyrus SASL, not distributed with Re

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

© [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](#) 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](#)