



CVE-2002-2074

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

Summary

CVE	CVE-2002-2074
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 Mailidx before 20020105 allows remote attackers to execute arbitrary SQL commands via the

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Erwin Lansing	Mailidx	20010925	All	All	All
Application	Erwin Lansing	Mailidx	20010925	All	All	All

References

Reference
dl.droso.net/mailidx-20020105.tar.gz
Erwin Lansing mailidx Input Validation Vulnerability
SecurityTracker.com Archives - Mailidx Perl-based Mailbox Front End Allows Remote Users to Execute SQL Commands on the Underlying SC
ISS X-Force Database: mailidx-search-input-validation (7965): mailidx search page fails to properly filter user-supplied input
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](#) 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](#).

Free CVE JSON API [cve.report/api](#)

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