



# CVE-2006-0224

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2006-0224                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | mitre                                                                                                                         |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2006-01-25 02:03:00 UTC                                                                                                       |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                       |
| Description     | Buffer overflow in Library of Assorted Spiffy Things (LibAST) 0.6.1 and earlier, as used in Eterm and possibly other software |

## Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

EPSS: 0.002160000 probability, percentile 0.442650000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|             |                        |                        |       |     |     |     |
|-------------|------------------------|------------------------|-------|-----|-----|-----|
| Application | <a href="#">Libast</a> | <a href="#">Libast</a> | 0.4   | All | All | All |
| Application | <a href="#">Libast</a> | <a href="#">Libast</a> | 0.5   | All | All | All |
| Application | <a href="#">Libast</a> | <a href="#">Libast</a> | 0.6   | All | All | All |
| Application | <a href="#">Libast</a> | <a href="#">Libast</a> | 0.6.1 | All | All | All |

Vendor Declared Affected Products

| Source | Vendor             | Product             | Version      | Platforms     |
|--------|--------------------|---------------------|--------------|---------------|
| CNA    | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

References

| Reference                                                                          | Source                               | Link                        |
|------------------------------------------------------------------------------------|--------------------------------------|-----------------------------|
| Eterm LibAST Library Local Buffer Overflow Vulnerability                           | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.secu</a>    |
| SecurityFocus                                                                      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.secu</a>    |
| mandriva.com                                                                       | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.manc</a>    |
| Rosiello Security - Eterm-LibAST Advisory - CXSecurity.com                         | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">securityrec</a> |
| www.rosiello.org/en/read_bugs.php                                                  | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.rosie</a>   |
| SecurityFocus                                                                      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.secu</a>    |
| Debian -- Security Information -- DSA-976-1 libast                                 | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.debia</a>   |
| Gentoo update for libast - Advisories - Secunia                                    | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">secunia.cc</a>  |
| Secunia - Advisories - LibAST Configuration Filename Buffer Overflow Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">secunia.cc</a>  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.vupe</a>    |
| LibAST: Privilege escalation (GLSA 200601-14) — Gentoo security                    | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.gent</a>    |
| IBM X-Force Exchange                                                               | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">exchange.</a>   |
| The Library of Assorted Spiffy Things – Freecode                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">freshmeat.</a>  |
| www.osvdb.org/22735                                                                | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.osvd</a>    |
| SecurityFocus                                                                      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.secu</a>    |
| About Secunia Research   Flexera                                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">secunia.cc</a>  |
| CVE Program record                                                                 | CVE.ORG                              | <a href="#">www.cve.c</a>   |
| NVD vulnerability detail                                                           | NVD                                  | <a href="#">nvd.nist.gc</a> |



No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)