



# CVE-2008-7223

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

## Summary

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2008-7223                                                                                                                    |
| State           | PUBLISHED                                                                                                                        |
| Assigner        | mitre                                                                                                                            |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                     |
| Published       | 2009-09-14 14:30:00 UTC                                                                                                          |
| Updated         | 2026-04-23 00:35:47 UTC                                                                                                          |
| Description     | Multiple cross-site scripting (XSS) vulnerabilities in LinPHA before 1.3.3 allow remote attackers to inject arbitrary web script |

## Risk And Classification

**Primary CVSS:** v2.0 4.3 from nvd@nist.gov

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

**Problem Types:** CWE-79 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Linpha | Linpha  | 0.9.0   | All    | All     | All      |

|             |                        |                        |       |       |     |     |
|-------------|------------------------|------------------------|-------|-------|-----|-----|
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 0.9.1 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 0.9.2 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 0.9.3 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 0.9.4 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.0   | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.0   | beta1 | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.0   | beta2 | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.0   | beta3 | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.0   | rc1   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.1.0 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.1.1 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.2.0 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.3.0 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | 1.3.1 | All   | All | All |
| Application | <a href="#">Linpha</a> | <a href="#">Linpha</a> | All   | All   | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |
|-----------------------------------|--------|---------|--------------|---------------|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |

| References                                                          |                                      |                                         |
|---------------------------------------------------------------------|--------------------------------------|-----------------------------------------|
| Reference                                                           | Source                               | Link                                    |
| Version 1.3.3 of LinPHA   freshmeat.net                             | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">freshmeat.net</a>           |
| LinPHA Multiple Cross-Site Scripting Vulnerabilities                | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.securityfocus.com</a>   |
| SourceForge.net CVS Repository - [linpha] View of /linpha/ChangeLog | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">linpha.cvs.sourceforge.</a> |
| osvdb.org/43191                                                     | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">osvdb.org</a>               |
| CVE Program record                                                  | CVE.ORG                              | <a href="#">www.cve.org</a>             |
| NVD vulnerability detail                                            | NVD                                  | <a href="#">nvd.nist.gov</a>            |

No vendor comments have been submitted for this CVE.

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

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)