



# CVE-2022-33009

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2022-33009  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-06-27 23:15:00 UTC   |
| <b>Updated</b>         | 2022-07-06 19:32:00 UTC   |
| <b>Description</b>     | A stored cross-site scripting (XSS) vulnerability in LightCMS v1.3.11 allows attackers to execute arbitrary web scripts or HT |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor           | Product  | Version | Update | Edition | Language |
|-------------|------------------|----------|---------|--------|---------|----------|
| Application | Lightcms Project | Lightcms | 1.3.11  | All    | All     | All      |

## References

| Reference   | Source  | Li                  |
|---|---------|---------------------|
| A stored cross-site scripting (XSS) vulnerability exists in LightCMS "contents" field · Issue #30 · eddy8/LightCMS · GitHub | MISC    | <a href="#">gi</a>  |
| GitHub - eddy8/LightCMS: LightCMS是一个基于Laravel开发的轻量级CMS系统，也可以作为一个通用的后台管理框架使用。  | MISC    | <a href="#">gi</a>  |
| Content Management System   LightCMS  | MISC    | <a href="#">lic</a> |
| CVE Program record  | CVE.ORG | <a href="#">w</a>   |
| NVD vulnerability detail  | NVD     | <a href="#">nv</a>  |

No vendor comments have been submitted for this CVE.

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

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)