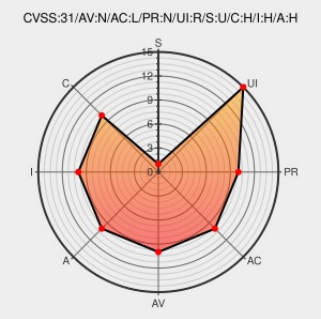
# CVE-2022-2540

Published on: Not Yet Published

Last Modified on: 01/11/2024 09:15:00 AM UTC

## CVE-2022-2540

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Link Optimizer Lite from Link Optimizer Lite Project contain the following vulnerability:

The Link Optimizer Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-Site Scripting in versions up to, and including 1.4.5. This is due to missing nonce validation on the admin_page function found in the ~/admin.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

CVE-2022-2540 has been assigned by security@wordfence.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **adambard** - **Link Optimizer Lite** version **<= 1.4.5**

### CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Vulnerability Advisories - Wordfence | www.wordfence.com text/html | MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-2540 |
| No Description Provided | www.wordfence.com | www.wordfence.com/threat-intel/vulnerabilities/id/ca64692b-b194-4ceb-975e-72e4041252f2?source=cve |
| 403 Forbidden | plugins.trac.wordpress.org text/html Inactive Link Not Archived | MISC plugins.trac.wordpress.org/browser/link-optimizer-lite/1.4.5/admin.php#L20 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Link Optimizer Lite Project | Link Optimizer Lite | All | All | All | All |

cpe:2.3:a:link_optimizer_lite_project:link_optimizer_lite:*:*:*:*:*:wordpress:*:*:

## Discovery Credit

Hayato Takizawa

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2022-2540 : The Link Optimizer Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery to Cross-S… twitter.com/i/web/status/1… | 2022-09-06 18:10:41 |
| @LinInfoSec | Wordpress - CVE-2022-2540: wordfence.com/vulnerability-… | 2022-09-06 21:01:01 |

← Previous ID

Next ID→



**CVE.report and Source URL Uptime Status status.cve.report**