



# Album and Image Gallery plus Lightbox <= 2.0 - Unauthenticated Arbitrary Shortcode Execution

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2024-4194  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | Wordfence  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2024-06-06 02:15:53 UTC  |
| <b>Updated</b>         | 2026-04-08 18:21:42 UTC  |
| <b>Description</b>     | The The Album and Image Gallery plus Lightbox plugin for WordPress is vulnerable to arbitrary shortcode execution in all v |

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

**Problem Types:** CWE-94 | NVD-CWE-noinfo | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

| Version | Source                 | Type      | Score | Severity | Vector                                       |
|---------|------------------------|-----------|-------|----------|--|
| 3.1     | nvd@nist.gov           | Primary   | 7.3   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L |
| 3.1     | security@wordfence.com | Secondary | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N |
| 3.1     | CNA                    | DECLARED  | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor          | Product                               | Version | Update | Edition | Language |
|-------------|-----------------|---------------------------------------|---------|--------|---------|----------|
| Application | Essentialplugin | Album And Image Gallery Plus Lightbox | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor          | Product                               | Version             | Platforms     |
|--------|-----------------|---------------------------------------|---------------------|---------------|
| CNA    | Essentialplugin | Album And Image Gallery Plus Lightbox | affected 2.0 semver | Not specified |
| ADP    | Wponlinesupport | Album And Image Gallery Plus Lightbox | affected 2.0 custom | Not specified |

### References

| Reference   | Source                               | Link  |
|---|--------------------------------------|---|
| plugins.trac.wordpress.org/changeset  | security@wordfence.com               | plugins.trac.wordpress.org/changeset  |
| plugins.trac.wordpress.org/browser/album-and-image-gallery-plus-lightbox/trunk/includes/... | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org/browser/album-and-image-gallery-plus-lightbox/trunk/includes/... |
| plugins.trac.wordpress.org/browser/album-and-image-gallery-plus-lightbox/trunk/includes/... | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org/browser/album-and-image-gallery-plus-lightbox/trunk/includes/... |
| www.wordfence.com/threat-intel/vulnerabilities/id/4822f1c7-3f83-416c-8957-17e4b...          | af854a3a-2127-422b-91ae-364da2661108 | www.wordfence.com/threat-intel/vulnerabilities/id/4822f1c7-3f83-416c-8957-17e4b...          |
| CVE Program record  | CVE.ORG                              | www.cve.org/CVE/entry/4822f1c7-3f83-416c-8957-17e4b...                                      |
| NVD vulnerability detail  | NVD                                  | nvd.nist.gov/vuln/detail/CVE-2024-4822  |

### Vendor Comments And Credit

Discovery Credit

**CNA:** Matthew Rollings (en)

### Additional Advisory Data

| Source | Time                     | Event     |
|--------|--------------------------|-----------|
| CNA    | 2024-06-05T00:00:00.000Z | Disclosed |

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](#)

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