



# Multiple Plugins <= (Various Versions) - Authenticated (Contributor+) Stored DOM-Based Cross-Site Scripting via prettyPhoto JavaScript Library

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

## Summary

<b>CVE</b>	CVE-2025-2540
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-07-03 12:15:24 UTC
<b>Updated</b>	2026-04-08 18:24:36 UTC
<b>Description</b>	Multiple plugins for WordPress are vulnerable to Stored Cross-Site Scripting via the plugin's bundled prettyPhoto library (ve

## Risk And Classification

**Primary CVSS:** v3.1 6.4 MEDIUM from security@wordfence.com

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

**EPSS:** 0.000970000 probability, percentile 0.267170000 (date 2026-04-08)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Nayon46</a>	<a href="#">Awesome Wp Image Gallery</a>	affected 1.0 semver	Not specified
CNA	<a href="#">Raihancse</a>	<a href="#">Awesome Gallery</a>	affected 1.0 semver	Not specified
CNA	<a href="#">Devrix</a>	<a href="#">Easy Image Gallery</a>	affected 1.5.2 semver	Not specified
CNA	<a href="#">Fuzzoid</a>	<a href="#">Easy 3D Viewer</a>	affected 1.8.6.6 semver	Not specified
CNA	<a href="#">Wptipsntricks</a>	<a href="#">WP Video Lightbox</a>	affected 1.9.11 semver	Not specified

### References

Reference	Source	Link
<a href="https://plugins.trac.wordpress.org/browser/woo-3d-viewer/trunk/includes/ext/prettyPhoto/js/jquery.prettyPhoto.js">plugins.trac.wordpress.org/browser/woo-3d-viewer/trunk/includes/ext/prettyPhoto/js/jquery...</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/browser/woo-3d-viewer/trunk/includes/ext/prettyPhoto/js/jquery.prettyPhoto.js">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/changeset/3266651/wp-video-lightbox">plugins.trac.wordpress.org/changeset/3266651/wp-video-lightbox</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/changeset/3266651/wp-video-lightbox">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/changeset/3282390/woo-3d-viewer">plugins.trac.wordpress.org/changeset/3282390/woo-3d-viewer</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/changeset/3282390/woo-3d-viewer">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/browser/awesome-wp-image-gallery/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordpress.org/browser/awesome-wp-image-gallery/trunk/js/jquery.prettyPhoto.js</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/browser/awesome-wp-image-gallery/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/changeset">plugins.trac.wordpress.org/changeset</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/changeset">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/browser/easy-image-gallery/trunk/includes/lib/prettyphoto/jquery.prettyPhoto.js">plugins.trac.wordpress.org/browser/easy-image-gallery/trunk/includes/lib/prettyphoto/jqu...</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/browser/easy-image-gallery/trunk/includes/lib/prettyphoto/jquery.prettyPhoto.js">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/browser/awesome-gallery/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordpress.org/browser/awesome-gallery/trunk/js/jquery.prettyPhoto.js</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/browser/awesome-gallery/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordp</a>
<a href="https://plugins.trac.wordpress.org/browser/wp-video-lightbox/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordpress.org/browser/wp-video-lightbox/trunk/js/jquery.prettyPhoto.js</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/browser/wp-video-lightbox/trunk/js/jquery.prettyPhoto.js">plugins.trac.wordp</a>
<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/82892be3-91d5-4350-96b0-dc68a...">www.wordfence.com/threat-intel/vulnerabilities/id/82892be3-91d5-4350-96b0-dc68a...</a>	security@wordfence.com	<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/82892be3-91d5-4350-96b0-dc68a...">www.wordfence.cc</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Craig Smith (en)

### Additional Advisory Data

Source	Time	Event
--------	------	-------

CNA	2025-03-19T00:00:00.000Z	Vendor Notified
CNA	2025-07-02T23:16:46.000Z	Disclosed

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)