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

CVE	CVE-2025-2540
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-03 12:15:24 UTC
Updated	2026-04-08 18:24:36 UTC
Description	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	Nayon46	Awesome Wp Image Gallery	affected 1.0 semver	Not specified
CNA	Raihancse	Awesome Gallery	affected 1.0 semver	Not specified
CNA	Devrix	Easy Image Gallery	affected 1.5.2 semver	Not specified
CNA	Fuzzoid	Easy 3D Viewer	affected 1.8.6.6 semver	Not specified
CNA	Wptipsntricks	WP Video Lightbox	affected 1.9.11 semver	Not specified

References

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

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.