



IMGspider <= 2.3.10 - Authenticated (Contributor+) Arbitrary File Upload via 'upload_img_file'

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

Summary

CVE	CVE-2024-6318
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-04 09:15:04 UTC
Updated	2026-04-08 17:19:10 UTC
Description	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_i

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security@wordfence.com

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

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wbolt	Imgspider	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wbolt	IMGspider	affected 2.3.10 semver	Not specified
ADP	Wbolt	Imgspider	affected 2.3.10 custom	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/306f00e4-9a70-48be-a91e-e3966...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/changeset/3107741/imgspider	af854a3a-2127-422b-91ae-364da2661108	plugins.t
plugins.trac.wordpress.org/browser/imgspider/tags/2.3.10/classes/post.class.php	af854a3a-2127-422b-91ae-364da2661108	plugins.t
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-25T00:00:00.000Z	Discovered
CNA	2024-06-25T00:00:00.000Z	Vendor Notified
CNA	2024-07-03T00:00:00.000Z	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](#)