Omnipress <= 1.6.5 - Authenticated (Author+) Stored Cross-Site Scripting

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-12163
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-05 06:16:06 UTC
Updated	2026-04-08 17:20:08 UTC
Description	The Omnipress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to,

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

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	Omnipressteam	Omnipress	affected 1.6.5 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/omnipress/tags/1.6.3/includes/RestApi/Controllers/V1/...	security@wordfence.com	plugins.trac.wordp
plugins.trac.wordpress.org/browser/omnipress/tags/1.6.3/includes/Core/RestControllersBas...	security@wordfence.com	plugins.trac.wordp
www.wordfence.com/threat-intel/vulnerabilities/id/15aabe3b-1b77-4e4e-9710-cf069...	security@wordfence.com	www.wordfence.c
plugins.trac.wordpress.org/browser/omnipress/tags/1.6.3/includes/uploader/FileUploader.php	security@wordfence.com	plugins.trac.wordp
owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload	security@wordfence.com	owasp.org
plugins.trac.wordpress.org/browser/omnipress/tags/1.6.3/includes/uploader/FileUploader.php	security@wordfence.com	plugins.trac.wordp
cwe.mitre.org/data/definitions/434.html	security@wordfence.com	cwe.mitre.org
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Kai Aizen (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-04T16:31:20.000Z	Disclosed

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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