ContentStudio <= 1.3.7 - Authenticated (Author+) Arbitrary File Upload

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

Summary

CVE	CVE-2025-12181
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 18:23:30 UTC
Description	The ContentStudio plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the cstu_

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

EPSS: 0.004570000 probability, percentile 0.639500000 (date 2026-04-08)

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

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Contentstudio	ContentStudio	affected 1.3.7 semver	Not specified

References

Reference	Source	Link
wordpress.org/plugins/contentstudio	security@wordfence.com	wordpress.org
plugins.trac.wordpress.org/changeset/3412182	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/5b92b0a4-7ebf-43b3-837b-ad710...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Kenneth Dunn (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-04T17:24:52.000Z	Disclosed

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