WordPress WP Calais Auto Tagger plugin <= 2.0 - CSRF to Stored XSS vulnerability

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

Summary

CVE	CVE-2025-32563
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-09 17:15:46 UTC
Updated	2026-04-23 15:29:06 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in dangrossman WP Calais Auto Tagger calais-auto-tagger allows Cross S

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from audit@patchstack.com

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

Problem Types: CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Changed

Confidentiality
Low

Integrity
Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dangrossman	WP Calais Auto Tagger	affected 2.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/calais-auto-tagger/vulnerability/wo...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

CNA: SOPROBRO | Patchstack Bug Bounty Program (en)

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