WordPress Push Notifications for WordPress by PushAssist plugin <= 3.0.8 - Arbitrary File Upload vulnerability

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

Summary

CVE	CVE-2024-52408
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-16 22:15:06 UTC
Updated	2026-04-23 15:21:06 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in pushassist Push Notifications for WordPress by PushAssis

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from audit@patchstack.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

vailability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pushassist	Push Notifications For WordPress By PushAssist	affected 3.0.8 custom	Not specified
ADP	Pushassist	Push Notifications	affected 3.0.8 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/push-notification-for-wp-by-pushass...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter | Patchstack Bug Bounty Program (en)

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