



WordPress WP Load Gallery Plugin <= 2.1.6 - Arbitrary File Upload vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-23942
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-22 15:15:26 UTC
Updated	2026-04-23 15:24:49 UTC

Description

Unrestricted Upload of File with Dangerous Type vulnerability in ngocuct0912 WP Load Gallery wp-load-gallery allows Uplo

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from audit@patchstack.com

CVSS:3.1/AV:N/AC:L/PR:H/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	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ngocuct0912	WP Load Gallery	affected 2.1.6 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/wp-load-gallery/vulnerability/wordp...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and



Vendor Comments And Credit

Discovery Credit

CNA: Le Ngoc Anh | Patchstack Bug Bounty Program (en)

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