WordPress FW Gallery plugin <= 8.0.0 - Arbitrary File Upload Vulnerability

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

Summary

CVE	CVE-2025-49414
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-04 12:15:30 UTC
Updated	2026-04-23 15:31:38 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in Fastw3b LLC FW Gallery fw-gallery allows Using Malicious

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from audit@patchstack.com

CVSS:3.1/AV:N/AC:L/PR:N/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	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Changed

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fastw3b LLC	FW Gallery	affected 8.0.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/fw-gallery/vulnerability/wordpress-...	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: LVT-tholv2k | Patchstack Bug Bounty Program (en)

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