WordPress BEAF plugin <= 4.6.10 - Arbitrary File Upload Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-47549
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-07 15:16:11 UTC
Updated	2026-04-01 17:24:02 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in Themefic BEAF beaf-before-and-after-gallery allows Uploa

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

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

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
High

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Themefic	Ultimate Before After Image Slider Gallery	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Themefic	BEAF	affected 4.6.10 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/beaf-before-and-after-gallery/vulne...	audit@patchstack.com	patchstack.com	Third Party Ac
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: Ryan Kozak | Patchstack Bug Bounty Program (en)

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