WordPress Anant Addons for Elementor plugin <= 1.1.8 - CSRF to Arbitrary Plugin Installation vulnerability

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

Summary

CVE	CVE-2025-32641
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-09 17:15:49 UTC
Updated	2026-04-23 15:29:15 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in anantaddons Anant Addons for Elementor anant-addons-for-elementor

Risk And Classification

Primary CVSS: v3.1 9.6 CRITICAL from audit@patchstack.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

ntegrity

High

vailability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Anantaddons	Anant Addons For Elementor	affected 1.1.8 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/anant-addons-for-elementor/vulnerab...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter | Patchstack Bug Bounty Program (en)

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