

WordPress ElementsCSS Addons for Elementor plugin <= 1.0.8.9 - Server Side Request Forgery (SSRF) vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2025-31796
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-01 15:16:17 UTC
Updated	2026-04-23 15:28:18 UTC
Description	Server-Side Request Forgery (SSRF) vulnerability in TheInnovs ElementsCSS Addons for Elementor css-for-elementor allc

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from audit@patchstack.com

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

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TheInnovs	ElementsCSS Addons For Elementor	affected 1.0.8.9 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/css-for-elementor/vulnerability/wor...	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: Tran Nguyen Bao Khanh (VCI - VNPT Cyber Immunity) | Patchstack Bug Bounty Program (en)

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