



# WordPress The Pack Elementor addons plugin <= 2.0.8.3 - Cross Site Request Forgery (CSRF) to XSS vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-32785
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-24 11:15:47 UTC
<b>Updated</b>	2026-04-28 19:24:57 UTC
<b>Description</b>	Cross-Site Request Forgery (CSRF) vulnerability in Webangon The Pack Elementor addons allows Cross-Site Scripting (XSS)

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.001260000 probability, percentile 0.315280000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**Required**

Scope

**Changed**

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Webangon</a>	<a href="#">The Pack Elementor Addons</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Webangon</a>	<a href="#">The Pack Elementor Addons</a>	affected n/a 2.0.8.3 custom	Not specified

#### References

Reference	Source	Link
<a href="https://patchstack.com/database/vulnerability/the-pack-addon/wordpress-the-pack-elem...">patchstack.com/database/vulnerability/the-pack-addon/wordpress-the-pack-elem...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://patchstack.com">patchstack.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Le Ngoc Anh (Patchstack Alliance) (en)

#### Additional Advisory Data

Solutions

**CNA:** Update to 2.0.8.4 or a higher version.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)