



# Envo's Elementor Templates & Widgets for WooCommerce <= 1.4.4 - Cross-Site Request Forgery via ajax\_plugin\_activation

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

## Summary

<b>CVE</b>	CVE-2024-0767
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-02-28 09:15:41 UTC
<b>Updated</b>	2026-04-08 19:19:16 UTC
<b>Description</b>	The Envo's Elementor Templates & Widgets for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) via the ajax_plugin_activation endpoint. An attacker can trigger the activation of a plugin without the user's consent, potentially leading to unauthorized actions or data exposure.

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from security@wordfence.com

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

**EPSS:** 0.001250000 probability, percentile 0.314650000 (date 2026-04-24)

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Envothemes	Envos Elementor Templates Widgets For Woocommerce	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Envothemes	Envos Templates Widgets For Elementor And WooCommerce	affected 1.4.4 semver	Not specified

### References

Reference	Source
www.wordfence.com/threat-intel/vulnerabilities/id/cca71257-05dc-43d5-8de6-faf0a...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/envo-elementor-for-woocommerce/trunk/includes/admin/i...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3041303/envo-elementor-for-woocommerce/trunk/includ...	security@wordfence.com
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

### Vendor Comments And Credit

Discovery Credit

**CNA:** Marco Wotschka (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-01-19T00:00:00.000Z	Discovered
CNA	2024-02-27T00:00:00.000Z	Disclosed

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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)