



# WPML Multilingual CMS <= 4.6.12 - Authenticated (Contributor+) Remote Code Execution via Twig Server-Side Template Injection

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

## Summary

<b>CVE</b>	CVE-2024-6386
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-08-21 21:15:08 UTC
<b>Updated</b>	2026-04-08 19:22:08 UTC
<b>Description</b>	The WPML plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.6.12 via Tw

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**EPSS:** 0.739110000 probability, percentile 0.988230000 (date 2026-04-13)

**Problem Types:** CWE-1336 | CWE-94 | CWE-1336 CWE-1336 Improper Neutralization of Special Elements Used in a Template Engine

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/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	Wpml	Wpml	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WPML	WPML	affected 4.6.12 semver	Not specified
ADP	Wpml	Wpml	affected 4.6.12 semver	Not specified

### References

Reference	Source	Link	Tags
sec.stealthcopter.com/wpml-rce-via-twig-ssti	security@wordfence.com	sec.stealthcopter.com	Exploit
www.wordfence.com/threat-intel/vulnerabilities/id/f7fc91cc-e529-4362-8269-bf7ee...	security@wordfence.com	www.wordfence.com	Threat Intel
wpml.org	security@wordfence.com	wpml.org	Product
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

### Vendor Comments And Credit

Discovery Credit

**CNA:** Matthew Rollings (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-06-19T00:00:00.000Z	Discovered
CNA	2024-08-21T08:00:14.000Z	Disclosed

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

---

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)