



# WPCafe – Online Food Ordering, Restaurant Menu, Delivery, and Reservations for WooCommerce <= 2.2.24 - Authenticated (Contributor+) Stored Cross-Site Scripting via Reservation Form Shortcode

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

## Summary

<b>CVE</b>	CVE-2024-5427
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-05-31 07:15:10 UTC
<b>Updated</b>	2026-04-08 18:22:03 UTC
<b>Description</b>	The WPCafe – Online Food Ordering, Restaurant Menu, Delivery, and Reservations for WooCommerce plugin for WordPre

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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="#">Themewinter</a>	<a href="#">Wpcafe</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Arraytics</a>	<a href="#">WPCafe Restaurant Menu Online Food Ordering Table Booking System</a>	affected 2.2.24 semver	Not specified

#### References

Reference	Source	Link
<a href="https://wordpress.org/plugins/wp-cafe">wordpress.org/plugins/wp-cafe</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">wp</a>
<a href="https://plugins.trac.wordpress.org/changeset/3095135">plugins.trac.wordpress.org/changeset/3095135</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">pli</a>
<a href="https://plugins.trac.wordpress.org/browser/wp-cafe/trunk/core/shortcodes/views/reservation/reser...">plugins.trac.wordpress.org/browser/wp-cafe/trunk/core/shortcodes/views/reservation/reser...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">pli</a>
<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/336e2429-97ab-4948-9d21-f0121...">www.wordfence.com/threat-intel/vulnerabilities/id/336e2429-97ab-4948-9d21-f0121...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">wp</a>
CVE Program record	CVE.ORG	<a href="#">wp</a>
NVD vulnerability detail	NVD	<a href="#">nv</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** [Krzysztof Zajac \(en\)](#)

#### Additional Advisory Data

Source	Time	Event
CNA	2024-05-30T18:20:55.000Z	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](#)