



# WordPress Woffice theme <= 5.4.14 - Unauthenticated Account Takeover vulnerability

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

## Summary

<b>CVE</b>	CVE-2024-43234
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-12-16 16:15:07 UTC
<b>Updated</b>	2026-04-01 16:17:41 UTC
<b>Description</b>	Authentication Bypass Using an Alternate Path or Channel vulnerability in WofficeIO Woffice woffice allows Authentication Bypass Using an Alternate Path or Channel

## Risk And Classification

**Problem Types:** CWE-288 | CWE-288 Authentication Bypass Using an Alternate Path or Channel

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xtendify	Woffice	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WofficeIO	Woffice	affected 5.4.14 custom	Not specified

## References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Theme/woffice/vulnerability/wordpress-woff...	audit@patchstack.com	patchstack.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

## Vendor Comments And Credit

Discovery Credit

**CNA:** Rafie Muhammad | Patchstack Bug Bounty Program (en)

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](#)