



WordPress AliExpress Dropshipping with AliNext Lite plugin <= 3.4.6 - CSRF to XSS vulnerability

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

Summary

CVE	CVE-2024-37213
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 14:15:12 UTC
Updated	2026-04-01 16:17:20 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in guru-aliexpress AliNext ali2woo-lite allows Cross Site Request Forgery.

Risk And Classification

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Guru-aliexpress	AliNext	affected 3.4.6 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/Wordpress/Plugin/ali2woo-lite/vulnerability/wordpres...	audit@patchstack.com	patchstack.cc
patchstack.com/database/vulnerability/ali2woo-lite/wordpress-aliexpress-drop...	af854a3a-2127-422b-91ae-364da2661108	patchstack.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Majed Refaea | 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](#).

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