



Cross-Site Request Forgery (CSRF) vulnerability in realmag777 BEAR and WOLF WordPress plugins

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

Summary

CVE	CVE-2024-31430
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-10 20:15:07 UTC
Updated	2026-04-28 19:24:28 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Profes

Risk And Classification

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

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

EPSS: 0.001660000 probability, percentile 0.373830000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	audit@patchstack.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	CVSS	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

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pluginus	Bear - Woocommerce Bulk Editor And Products Manager Professional	All	All	All	All
Application	Pluginus	Wolf - Wordpress Posts Bulk Editor And Products Manager Professional	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Realmag777	WOLF WordPress Posts Bulk Editor And Manager Professional	affected n/a 1.0.8.1 cu
CNA	Realmag777	BEAR Bulk Editor And Products Manager Professional For WooCommerce By Pluginus.Net	affected n/a 1.1.4.1 cu

References

Reference	Source	Link
patchstack.com/database/vulnerability/bulk-editor/wordpress-wolf-wordpress-p...	af854a3a-2127-422b-91ae-364da2661108	patchstack.co
patchstack.com/database/vulnerability/woo-bulk-editor/wordpress-bear-bulk-ed...	af854a3a-2127-422b-91ae-364da2661108	patchstack.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Dhabaleshwar Das (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update WOLF plugin to 1.0.8.2 or a higher version. Update BEAR plugin to 1.1.4.2 or a higher version.

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](#)