



WordPress WooCommerce AWeber Newsletter Subscription plugin <= 4.0.2 - Unauthenticated Access Token Change/Reset vulnerability

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

Summary

CVE CVE-2024-33944**State** PUBLISHED**Assigner** Patchstack**Source Priority** CVE Program / NVD first with legacy fallback**Published** 2024-05-02 13:15:26 UTC**Updated** 2026-04-28 19:25:17 UTC**Description** Missing Authorization vulnerability in Kestrel WooCommerce AWeber Newsletter Subscription. This issue affects WooComr

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from audit@patchstack.com**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L**EPSS:** 0.001270000 probability, percentile 0.315890000 (date 2026-04-28)**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kestrel	WooCommerce AWeber Newsletter Subscription	affected n/a 4.0.2 custom	Not specified
ADP	Kestrel Woocommerce	Awber Newsletter Subscription	affected - 4.0.2 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/woocommerce-aweber-newsletter-subscrip...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Dave Jong (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 4.0.3 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](#)