



WordPress Product Feed for WooCommerce plugin <= 2.3.1 - Broken Access Control vulnerability

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-66089 |
| State | PUBLISHED |
| Assigner | Patchstack |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-11-21 13:15:50 UTC |
| Updated | 2026-04-27 18:16:35 UTC |
| Description | Missing Authorization vulnerability in WebToffee Product Feed for WooCommerce webtoffee-product-feed allows Exploiting |

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.000200000 probability, percentile 0.054370000 (date 2026-04-27)

Problem Types: CWE-862 | CWE-862 Missing Authorization

| Version | Source | Type | Score | Severity | Vector |
|---------|----------------------|-----------|-------|----------|--|
| 3.1 | audit@patchstack.com | Secondary | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |
| 3.1 | CNA | CVSS | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------------------------|--|-----------------------|---------------|
| CNA | WebToffee | Product Feed For WooCommerce | affected 2.3.1 custom | Not specified |

References

| Reference | Source | Link | Tags |
|---|--|--|----------------|
| patchstack.com/database/Wordpress/Plugin/webtoffee-product-feed/vulnerabilit... | audit@patchstack.com | patchstack.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, and |

Vendor Comments And Credit

Discovery Credit

CNA: Legion Hunter | 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