



WordPress WPC Product Bundles for WooCommerce Plugin <= 7.3.1 is vulnerable to Cross Site Request Forgery (CSRF)

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-52127 |
| State | PUBLISHED |
| Assigner | Patchstack |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-01-05 09:15:09 UTC |
| Updated | 2026-04-28 19:22:58 UTC |
| Description | Cross-Site Request Forgery (CSRF) vulnerability in WPClever WPC Product Bundles for WooCommerce. This issue affects |

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: 0.000700000 probability, percentile 0.213480000 (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

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 | Wpclever | Wpc Product Bundles For Woocommerce | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|----------|-------------------------------------|---------------------------|---------------|
| CNA | WPClever | WPC Product Bundles For WooCommerce | affected n/a 7.3.1 custom | Not specified |

References

| Reference | Source | Link |
|---|--------------------------------------|-----------------------------|
| patchstack.com/database/vulnerability/woo-product-bundle/wordpress-wpc-produ... | af854a3a-2127-422b-91ae-364da2661108 | patchstack |
| CVE Program record | CVE.ORG | www.cve.o |
| NVD vulnerability detail | NVD | nvd.nist.go |

Vendor Comments And Credit

Discovery Credit

CNA: Brandon Roldan (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 7.3.2 or a higher version.

There are currently no legacy QID mappings associated with this CVE.

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