



# WordPress Blocksy Companion plugin <= 2.0.28 - Cross Site Request Forgery (CSRF) vulnerability

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2024-31932  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Patchstack  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2024-04-11 13:15:54 UTC   |
| <b>Updated</b>         | 2026-04-28 19:24:30 UTC   |
| <b>Description</b>     | Cross-Site Request Forgery (CSRF) vulnerability in CreativeThemes Blocksy Companion.This issue affects Blocksy Comp |

## 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:** 0.001160000 probability, percentile 0.299800000 (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 | 5.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 5.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |

## 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 | <a href="#">Creativethemes</a> | <a href="#">Blocksy Companion</a> | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor                         | Product                           | Version                    | Platforms     |
|--------|--------------------------------|-----------------------------------|----------------------------|---------------|
| CNA    | <a href="#">CreativeThemes</a> | <a href="#">Blocksy Companion</a> | affected n/a 2.0.28 custom | Not specified |

### References

| Reference   | Source                               | Link  |
|---|--------------------------------------|---|
| <a href="https://patchstack.com/database/vulnerability/blocksy-companion/wordpress-blocksy-co...">patchstack.com/database/vulnerability/blocksy-companion/wordpress-blocksy-co...</a> | af854a3a-2127-422b-91ae-364da2661108 | <a href="https://patchstack.com">patchstack.com</a> |
| CVE Program record  | CVE.ORG                              | <a href="https://www.cve.org">www.cve.org</a>       |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     |

### Vendor Comments And Credit

Discovery Credit

**CNA:** FearZzZz (Patchstack Alliance) (en)

### Additional Advisory Data

Solutions

**CNA:** Update to 2.0.29 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)