



# WordPress Verbosa theme <= 1.2.3 - Cross Site Scripting (XSS) vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2024-44050                                                                                                               |
| State           | PUBLISHED                                                                                                                    |
| Assigner        | Patchstack                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                 |
| Published       | 2024-09-17 23:15:20 UTC                                                                                                      |
| Updated         | 2026-04-23 15:19:04 UTC                                                                                                      |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cryout-creations Verbo |

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov         | Primary   | 5.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N |
| 3.1     | audit@patchstack.com | Secondary | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |

| CVSS v3.1 Breakdown |          |
|---------------------|----------|
| Attack Vector       | Network  |
| Attack Complexity   | Low      |
| Privileges Required | Low      |
| User Interaction    | Required |
| Scope               | Changed  |
| Confidentiality     |          |

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor          | Product | Version | Update | Edition | Language |
|-------------|-----------------|---------|---------|--------|---------|----------|
| Application | Cryoutcreations | Verbosa | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor           | Product | Version               | Platforms     |
|--------|------------------|---------|-----------------------|---------------|
| CNA    | Cryout-creations | Verbosa | affected 1.2.3 custom | Not specified |

References

| Reference                                                                       | Source               | Link           | Tags         |
|---------------------------------------------------------------------------------|----------------------|----------------|--------------|
| patchstack.com/database/Wordpress/Theme/verbosa/vulnerability/wordpress-verb... | audit@patchstack.com | patchstack.com |              |
| CVE Program record                                                              | CVE.ORG              | www.cve.org    | canonical    |
| NVD vulnerability detail                                                        | NVD                  | nvd.nist.gov   | canonical, s |

Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter | Patchstack Bug Bounty Program (en)

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