



# WordPress Simple Long Form Plugin <= 2.2.2 is vulnerable to Cross Site Scripting (XSS)

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2023-41136                                                                                                             |
| State           | PUBLISHED                                                                                                                  |
| Assigner        | Patchstack                                                                                                                 |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                               |
| Published       | 2023-11-30 12:15:07 UTC                                                                                                    |
| Updated         | 2026-04-28 19:21:14 UTC                                                                                                    |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Laurence/OhMyBox.Ini |

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-79 | 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   | 4.8   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N |
| 3.1     | audit@patchstack.com | Secondary | 5.9   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 5.9   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/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 | Ohmybox | Simple Long Form | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor               | Product          | Version                   | Platforms     |
|--------|----------------------|------------------|---------------------------|---------------|
| CNA    | LaurenceOhMyBox.info | Simple Long Form | affected n/a 2.2.2 custom | Not specified |

References

| Reference                                                                                          | Source                            |
|----------------------------------------------------------------------------------------------------|-----------------------------------|
| WordPress Simple Long Form plugin <= 2.2.2 - Cross Site Scripting (XSS) vulnerability - Patchstack | af854a3a-2127-422b-91ae-364da2661 |
| CVE Program record                                                                                 | CVE.ORG                           |
| NVD vulnerability detail                                                                           | NVD                               |

Vendor Comments And Credit

Discovery Credit

CNA: DoYeon Park / p6rkdoye0n (Patchstack Alliance) (en)

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