



GiveWP – Donation Plugin and Fundraising Platform <= 3.6.1 -- Authenticated(Contributor+) Stored Cross-Site Scripting via Shortcode

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2024-1957 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-04-13 02:15:06 UTC |
| Updated | 2026-04-08 18:20:54 UTC |
| Description | The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting |

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 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 | security@wordfence.com | Secondary | 6.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |
| 3.1 | CNA | DECLARED | 6.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N |

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 | Givewp | Givewp | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|-----------|---|-----------------------|---------------|
| CNA | Stellarwp | GiveWP Donation Plugin And Fundraising Platform | affected 3.6.1 semver | Not specified |

References

| Reference | Source | Link |
|--|--------------------------------------|------------|
| www.wordfence.com/threat-intel/vulnerabilities/id/61901d83-0d05-4be8-a318-43bea... | af854a3a-2127-422b-91ae-364da2661108 | www.v... |
| plugins.trac.wordpress.org/changeset/3068610/give/tags/3.7.0/includes/shortcodes.php | af854a3a-2127-422b-91ae-364da2661108 | plugins... |
| CVE Program record | CVE.ORG | www.c... |
| NVD vulnerability detail | NVD | nvd.nis... |

Vendor Comments And Credit

Discovery Credit

CNA: Ngô Thiên An (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|-----------|
| CNA | 2024-04-12T00:00:00.000Z | Disclosed |

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