# Webico Slider Flatsome Addons <= 2.0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via wbc_image Shortcode

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2024-5881 |
| **State** | PUBLISHED |
| **Assigner** | Wordfence |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2024-07-09 08:15:10 UTC |
| **Updated** | 2026-04-08 18:22:14 UTC |
| **Description** | The Webico Slider Flatsome Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wbc_ |

## Risk And Classification

**Primary CVSS:** v3.1 6.4 MEDIUM from security@wordfence.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/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 | 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
None

Scope
Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Tranbinhcse | Webico Slider Flatsome Addons | affected 2.0.1 semver | Not specified |

## References

| Reference | Source | I |
|---|---|---|
| plugins.trac.wordpress.org/browser/webico-slider-flatsome-addons/trunk/shortcodes/wbc_sl... | af854a3a-2127-422b-91ae-364da2661108 | p |
| www.wordfence.com/threat-intel/vulnerabilities/id/71eeddf4-5693-41bc-93ad-3c93d... | af854a3a-2127-422b-91ae-364da2661108 | v |
| CVE Program record | CVE.ORG | v |
| NVD vulnerability detail | NVD | r |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Francesco Carlucci (en)

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| CNA | 2024-07-08T19:37:49.000Z | Disclosed |

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 registred 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