



# Testimonial Carousel For Elementor <= 10.2.2 - Authenticated (Contributor+) Stored Cross-Site Scripting

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

| Summary         |                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2024-2253                                                                                                             |
| State           | PUBLISHED                                                                                                                 |
| Assigner        | Wordfence                                                                                                                 |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                              |
| Published       | 2024-05-30 04:15:09 UTC                                                                                                   |
| Updated         | 2026-04-08 19:21:01 UTC                                                                                                   |
| Description     | The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via URL values 1 |

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

**EPSS:** 0.002730000 probability, percentile 0.507580000 (date 2026-04-12)

**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

Integrity

Low

Availability

None

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

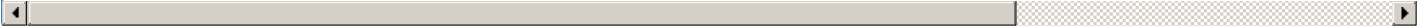


Vendor Declared Affected Products

| Source | Vendor | Product                            | Version                | Platforms     |
|--------|--------|------------------------------------|------------------------|---------------|
| CNA    | Uapp   | Testimonial Carousel For Elementor | affected 10.2.2 semver | Not specified |

References

| Reference                                                                                   | Source                               | Link                                                                                        |
|---------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------|
| plugins.trac.wordpress.org/changeset                                                        | security@wordfence.com               | plugins.trac.wordpress.org/changeset                                                        |
| www.wordfence.com/threat-intel/vulnerabilities/id/d559b862-ee07-4207-8c64-81961...          | af854a3a-2127-422b-91ae-364da2661108 | www.wordfence.com/threat-intel/vulnerabilities/id/d559b862-ee07-4207-8c64-81961...          |
| plugins.trac.wordpress.org/browser/testimonials-carousel-elementor/trunk/widgets/testimo... | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org/browser/testimonials-carousel-elementor/trunk/widgets/testimo... |
| CVE Program record                                                                          | CVE.ORG                              | CVE Program record                                                                          |
| NVD vulnerability detail                                                                    | NVD                                  | NVD vulnerability detail                                                                    |



Vendor Comments And Credit

Discovery Credit

**CNA:** Francesco Carlucci (en)

Additional Advisory Data

| Source | Time                     | Event     |
|--------|--------------------------|-----------|
| CNA    | 2024-05-29T00:00:00.000Z | Disclosed |

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

