



Chat Bubble <= 2.3 - Authenticated (Administrator+) Stored Cross-Site Scripting

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2024-0898 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-03-13 16:15:15 UTC |
| Updated | 2026-04-08 19:19:18 UTC |
| Description | The Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back plugin for Word |

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

EPSS: 0.001900000 probability, percentile 0.409390000 (date 2026-04-16)

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 | security@wordfence.com | Secondary | 4.4 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N |
| 3.1 | CNA | DECLARED | 4.4 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N |

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 | Bluecoral | Chat Bubble | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------|--|-------------------|
| CNA | Bluecoral | Chat Bubble Floating Chat With Contact Chat Icons Messages Telegram Email SMS Call Me Back | affected 2.3 semv |

References

| Reference | Source | Link |
|--|--------------------------------------|------------|
| wordpress.org/plugins/chat-bubble | af854a3a-2127-422b-91ae-364da2661108 | wordpress |
| www.wordfence.com/threat-intel/vulnerabilities/id/a56772fd-f77f-4ba5-b5c4-79ac8... | af854a3a-2127-422b-91ae-364da2661108 | www.worc |
| CVE Program record | CVE.ORG | www.cve.c |
| NVD vulnerability detail | NVD | nvd.nist.g |

Vendor Comments And Credit

Discovery Credit

CNA: Dikshita Trivedi (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|-----------|
| CNA | 2024-02-27T00:00:00.000Z | Disclosed |

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

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 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