# WordPress <= 6.8.2 - (Contributor+) Sensitive Data Exposure Vulnerability

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2025-58246 |
| **State** | PUBLISHED |
| **Assigner** | Patchstack |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2025-09-23 18:15:37 UTC |
| **Updated** | 2026-04-28 19:34:06 UTC |
| **Description** | Insertion of Sensitive Information Into Sent Data vulnerability in WordPress allows Retrieve Embedded Sensitive Data. The |

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from audit@patchstack.com

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

**EPSS:** 0.000390000 probability, percentile 0.118490000 (date 2026-04-28)

**Problem Types:** CWE-201 | CWE-201 CWE-201 Insertion of Sensitive Information Into Sent Data

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | audit@patchstack.com | Secondary | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |
| 3.1 | CNA | CVSS | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | WordPress | WordPress | affected 6.8 6.8.2 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.7 6.7.3 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.6 6.6.3 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.5 6.5.6 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.4 6.4.6 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.3 6.3.6 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.2 6.2.7 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.1 6.1.8 custom | Not specified |
| CNA | WordPress | WordPress | affected 6.0 6.0.10 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.9 5.9.11 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.8 5.8.11 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.7 5.7.13 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.6 5.6.15 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.5 5.5.16 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.4 5.4.17 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.3 5.3.19 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.2 5.2.22 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.1 5.1.20 custom | Not specified |
| CNA | WordPress | WordPress | affected 5.0 5.0.23 custom | Not specified |
| CNA | WordPress | WordPress | affected 4.9 4.9.27 custom | Not specified |
| CNA | WordPress | WordPress | affected 4.8 4.8.26 custom | Not specified |
| CNA | WordPress | WordPress | affected 4.7 4.7.30 custom | Not specified |

## References

| Reference |
|---|
| wordpress.org/news/2025/09/wordpress-6-8-3-release |
| patchstack.com/database/wordpress/wordpress/wordpress/vulnerability/wordpres... |

https://patchstack.com/database/wordpress/wordpress/wordpress/vulnerability/wordpress-wordpress-wordpress-6-8-2-sensitive-data-exposure

CVE Program record

NVD vulnerability detail

## Vendor Comments And Credit

Discovery Credit

**CNA:** Abu Hurayra (Patchstack Bug Bounty Program) (en)

**CNA:** John Blackbourn (WordPress core security team lead) (en)

**CNA:** Timothy Jacobs (en)

**CNA:** Peter Wilson (en)

**CNA:** Mike Nelson (en)

## Additional Advisory Data

Solutions

**CNA:** Update WordPress to one of the following patched or higher versions: 6.8.3, 6.7.4, 6.6.4, 6.5.7, 6.4.7, 6.3.7, 6.2.8, 6.1.9, 6.0.11, 5.9.12, 5.8.12, 5.7.14, 5.6.16, 5.5.17, 5.4.18, 5.3.20, 5.2.23, 5.1.21, 5.0.24, 4.9.28, 4.8.27, or 4.7.31.

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