



WP Customer Reviews <= 3.6.6 - Authenticated (Subscriber+) Sensitive Information Exposure

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-4686 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-11-22 16:15:09 UTC |
| Updated | 2026-04-08 17:17:04 UTC |
| Description | The WP Customer Reviews plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and inc |

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-862 | NVD-CWE-noinfo | CWE-862 CWE-862 Missing Authorization

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |
| 3.1 | security@wordfence.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 | DECLARED | 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

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------|---------------------|---------|--------|---------|----------|
| Application | Gowebolutions | Wp Customer Reviews | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|---------------------|-----------------------|---------------|
| CNA | Bompus | WP Customer Reviews | affected 3.6.6 semver | Not specified |
| ADP | Bompus | Wp Customer Reviews | affected 3.6.6 custom | Not specified |

References

| Reference | Source |
|---|--------------------------------------|
| plugins.trac.wordpress.org/changeset/2965656/wp-customer-reviews/trunk | af854a3a-2127-422b-91ae-364da2661108 |
| plugins.trac.wordpress.org/browser/wp-customer-reviews/trunk/include/admin/wp-customer-r... | af854a3a-2127-422b-91ae-364da2661108 |
| www.wordfence.com/threat-intel/vulnerabilities/id/24b9984c-ec33-4492-815b-67a21... | af854a3a-2127-422b-91ae-364da2661108 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

Vendor Comments And Credit

Discovery Credit

CNA: Marco Wotschka (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|------------|
| CNA | 2023-08-31T00:00:00.000Z | Discovered |
| CNA | 2023-10-31T00:00:00.000Z | Disclosed |

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

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 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