



# Profile Extra Fields by BestWebSoft <= 1.2.7 - Missing Authorization to Sensitive Information Exposure

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-4469  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | Wordfence  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-10-06 10:15:18 UTC  |
| <b>Updated</b>         | 2026-04-08 18:18:14 UTC  |
| <b>Description</b>     | The Profile Extra Fields by BestWebSoft plugin for WordPress is vulnerable to unauthorized access of data due to a missing |

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from security@wordfence.com

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

**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

| Version | Source                 | Type      | Score | Severity | Vector                                       |
|---------|------------------------|-----------|-------|----------|--|
| 3.1     | security@wordfence.com | Secondary | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 3.1     | CNA                    | DECLARED  | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/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 | Bestwebsoft | Profile Extra Fields | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor      | Product                             | Version               | Platforms     |
|--------|-------------|-------------------------------------|-----------------------|---------------|
| CNA    | Bestwebsoft | Profile Extra Fields By BestWebSoft | affected 1.2.7 semver | Not specified |

### References

| Reference  | Source                          |
|--|---------------------------------|
| 403 Forbidden  | af854a3a-2127-422b-91ae-364da26 |
| Profile Extra Fields by BestWebSoft <= 1.2.7 - Missing Authorization to Sensitive Information Exposure | af854a3a-2127-422b-91ae-364da26 |
| CVE Program record   | CVE.ORG                         |
| NVD vulnerability detail   | NVD                             |

### Vendor Comments And Credit

Discovery Credit

**CNA:** Alex Thomas (en)

### Additional Advisory Data

| Source | Time                     | Event           |
|--------|--------------------------|-----------------|
| CNA    | 2023-08-21T00:00:00.000Z | Discovered      |
| CNA    | 2023-10-03T00:00:00.000Z | Vendor Notified |
| CNA    | 2023-10-05T00:00:00.000Z | 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 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)