



BEAR <= 1.1.3.3 - Cross-Site Request Forgery to Product Deletion

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-4926 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-20 08:15:12 UTC |
| Updated | 2026-04-08 19:18:39 UTC |
| Description | The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due |

Risk And Classification

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

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

EPSS: 0.000690000 probability, percentile 0.212770000 (date 2026-04-09)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 4.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N |
| 3.1 | security@wordfence.com | Secondary | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |
| 3.1 | CNA | DECLARED | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|--|---------|--------|---------|----------|
| Application | Pluginus | Bear - Woocommerce Bulk Editor And Products Manager Professional | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|------------|--|-----------------------|
| CNA | Realmag777 | BEAR Bulk Editor And Products Manager Professional For WooCommerce By Pluginus.Net | affected 1.1.3.3 semv |

References

| Reference | Source | Link |
|--|--------------------------------------|--|
| BEAR <= 1.1.3.3 - Cross-Site Request Forgery to Product Deletion | af854a3a-2127-422b-91ae-364da2661108 | www.wordfence.com |
| 403 Forbidden | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org |
| 403 Forbidden | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

Vendor Comments And Credit

Discovery Credit

CNA: Marco Wotschka (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|------------|
| CNA | 2023-09-12T00:00:00.000Z | Discovered |
| CNA | 2023-09-25T00:00:00.000Z | Disclosed |

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

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)