



# Snippet Shortcodes <= 4.1.4 - Cross-Site Request Forgery

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2024-4543                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| State           | PUBLISHED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Assigner        | Wordfence                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Published       | 2024-07-03 05:15:10 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Updated         | 2026-04-08 17:18:55 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description     | The Snippet Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including 4.1.4. An attacker can exploit this vulnerability to perform actions on behalf of the authenticated user, such as changing the user's password, or deleting the user's account. This vulnerability can be exploited by an attacker who has access to the user's session ID, which can be obtained through a variety of means, including phishing, social engineering, or a previous security breach. The attacker can then use the session ID to perform actions on behalf of the user, such as changing the user's password, or deleting the user's account. This vulnerability can be exploited by an attacker who has access to the user's session ID, which can be obtained through a variety of means, including phishing, social engineering, or a previous security breach. |

| Risk And Classification                                                    |                        |           |       |          |                                              |
|----------------------------------------------------------------------------|------------------------|-----------|-------|----------|----------------------------------------------|
| Primary CVSS: v3.1 4.3 MEDIUM from security@wordfence.com                  |                        |           |       |          |                                              |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N                               |                        |           |       |          |                                              |
| Problem Types: CWE-352   CWE-352 CWE-352 Cross-Site Request Forgery (CSRF) |                        |           |       |          |                                              |
| Version                                                                    | Source                 | Type      | Score | Severity | Vector                                       |
| 3.1                                                                        | security@wordfence.com | Secondary | 4.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N |
| 3.1                                                                        | CNA                    | DECLARED  | 4.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N |

| 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)

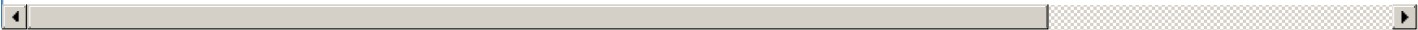
| Type        | Vendor | Product            | Version | Update | Edition | Language |
|-------------|--------|--------------------|---------|--------|---------|----------|
| Application | Yeken  | Snippet Shortcodes | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor  | Product            | Version               | Platforms     |
|--------|---------|--------------------|-----------------------|---------------|
| CNA    | Aliakro | Snippet Shortcodes | affected 4.1.4 semver | Not specified |

References

| Reference                                                                          | Source                               | Link                                                                                               |
|------------------------------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------|
| plugins.trac.wordpress.org/changeset/3110951                                       | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">plugins.trac.wordpress.org/changeset/3110951</a>                                       |
| www.wordfence.com/threat-intel/vulnerabilities/id/127b20c4-cd7c-4d04-b32f-bcc26... | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.wordfence.com/threat-intel/vulnerabilities/id/127b20c4-cd7c-4d04-b32f-bcc26...</a> |
| CVE Program record                                                                 | CVE.ORG                              | <a href="#">www.cve.org</a>                                                                        |
| NVD vulnerability detail                                                           | NVD                                  | <a href="#">nvd.nist.gov</a>                                                                       |



Vendor Comments And Credit

Discovery Credit

CNA: Benedictus Jovan (en)

Additional Advisory Data

| Source | Time                     | Event     |
|--------|--------------------------|-----------|
| CNA    | 2024-07-02T00:00:00.000Z | 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](#)

