



WP Fastest Cache <= 1.1.2 - Cross-Site Request Forgery via 'deleteCssAndJsCacheToolbar'

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-1927 |
| State | PUBLISHED |
| Assigner | Wordfence |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-04-06 21:15:07 UTC |
| Updated | 2026-04-08 18:17:56 UTC |
| Description | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, |

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

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 | 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 | Wpfastestcache | Wp Fastest Cache | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------------------------|---|-----------------------|---------------|
| CNA | Emrevona | WP Fastest Cache WordPress Cache Plugin | affected 1.1.2 semver | Not specified |

References

| Reference | Source | Link | Tags |
|---------------------------------------|--------------------------------------|---|----------------------|
| 403 Forbidden | af854a3a-2127-422b-91ae-364da2661108 | plugins.trac.wordpress.org | Patch |
| Not Found | af854a3a-2127-422b-91ae-364da2661108 | www.wordfence.com | Third Party Advisory |
| WordPress Security Plugin Wordfence | MITRE | wordfence.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: [Marco Wotschka \(en\)](#)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|-----------------|
| CNA | 2023-03-30T00:00:00.000Z | Discovered |
| CNA | 2023-04-03T00:00:00.000Z | Vendor Notified |
| CNA | 2023-04-06T00:00:00.000Z | Disclosed |

Legacy QID Mappings

[150671](#) WordPress WP Fastest Cache Plugin: Prior to 1.1.2 Multiple Security Vulnerabilities

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