



# WP Fastest Cache <= 0.9.0.2 - Authenticated (Subscriber+) Arbitrary File Deletion

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

## Summary

<b>CVE</b>	CVE-2020-36836
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-16 07:15:08 UTC
<b>Updated</b>	2026-04-08 18:17:12 UTC
<b>Description</b>	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized arbitrary file deletion in versions up to, and inclu

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from nvd@nist.gov

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

**EPSS:** 0.373590000 probability, percentile 0.971930000 (date 2026-04-22)

**Problem Types:** CWE-352 | CWE-22 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
3.1	security@wordfence.com	Primary	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

#### 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 0.9.0.3 semver	Not specified
ADP	Wpfastestcache	Wp Fastest Cache	affected 0.9.0.3 semver	Not specified

#### References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/2235160/wp-fastest-cache	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/82f80916-37ab-4c5a-9787-2544c...	security@wordfence.com	www.wordfence.com
wearetradecraft.com/advisories/tc-2020-0001	security@wordfence.com	wearetradecraft.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Glyn Wintle (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2020-02-05T00:00:00.000Z	Disclosed

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

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)