



# CVE-2021-24870

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-24870  |
| <b>State</b>           | RESERVED  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2024-01-16 16:15:00 UTC   |
| <b>Updated</b>         | 2024-01-19 15:25:00 UTC   |
| <b>Description</b>     | ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new |

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor         | Product          | Version | Update | Edition | Language |
|-------------|----------------|------------------|---------|--------|---------|----------|
| Application | Wpfastestcache | Wp Fastest Cache | All     | All    | All     | All      |

## References

| Reference   | Source  | Link  | Tags                     |
|---|---------|---|--------------------------|
| WP Fastest Cache < 0.9.5 - CSRF to Stored Cross-Site Scripting WordPress Security Vulnerability |         | <a href="https://wpscan.com">wpscan.com</a>     | Third Party              |
| Multiple vulnerabilities in WP Fastest Cache plugin   |         | <a href="https://jetpack.com">jetpack.com</a>   | Exploit, Third Party     |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>   | canonical                |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a> | canonical, authoritative |

No vendor comments have been submitted for this CVE.

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

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)