



CVE-2021-36850

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-36850 |
| State | PUBLIC |
| Assigner | audit@patchstack.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-10-04 17:15:00 UTC |
| Updated | 2021-10-08 17:31:00 UTC |
| Description | Cross-Site Request Forgery (CSRF) vulnerability in WordPress Media File Renamer – Auto & Manual Rename plugin (vers |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|---|---------|--------|---------|----------|
| Application | Meowapps | Media File Renamer - Auto Manual Rename | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|--|
| Media File Renamer – Auto & Manual Rename – WordPress plugin WordPress.org | CONFIRM | wordpress.org |
| WordPress Media File Renamer plugin <= 5.1.9 - Cross-Site Request Forgery (CSRF) vulnerability - Patchstack | MISC | patchstack.co |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

Vendor Comments And Credit

Discovery Credit

LEGACY: Original researcher - Ngo Van Thien (Patchstack Red Team)

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