



CVE-2021-36804

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

Summary

| | |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2021-36804 |
| State | PUBLIC |
| Assigner | cve@rapid7.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-08-04 23:15:00 UTC |
| Updated | 2021-08-13 13:30:00 UTC |
| Description | Akaunting version 2.1.12 and earlier suffers from a password reset spoofing vulnerability, wherein an attacker can proxy pa |

Risk And Classification

Problem Types: CWE-640

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | Akaunting | Akaunting | All | All | All | All |

References

| Reference | Source |
|-----------------------------------------------------------------------------------------------------------------------------------|--------|
| Host Injection Analyzer Enlightn | MISC |
| [8.x] Uncomment TrustHosts middleware to enable it by default by DanielCoulbourne · Pull Request #5477 · laravel/laravel · GitHub | MISC |
| Multiple Open Source Web App Vulnerabilities Fixed Rapid7 Blog | MISC |
| CVE Program record | CVE.OI |
| NVD vulnerability detail | NVD |

Vendor Comments And Credit

Discovery Credit

LEGACY: Wiktor Sędkowski of Nokia and Trevor Christiansen of Rapid7 discovered and reported this issue through Rapid7's vulnerability disclosure program.

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)