



CVE-2023-38874

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

Summary

CVE	CVE-2023-38874
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-28 04:15:00 UTC
Updated	2023-10-02 18:35:00 UTC
Description	A remote code execution (RCE) vulnerability via an insecure file upload exists in gugoan's Economizzer v.0.9-beta1 and co

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Economizzer	Economizzer	0.9	beta1	All	All
Application	Economizzer	Economizzer	april_2023	All	All	All

References

Reference	Source	Link	Tags
GitHub - gugoan/economizzer: Open Source Personal Finance Manager	MISC	github.com	
CVE-2023-38874: RCE in gugaan's Economizzer	MISC	github.com	
Economizzer - Open Source Personal Finance Manager	MISC	www.economizzer.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995456](#) PHP (Composer) Security Update for gugoan/economizzer (GHSA-pq98-6hf6-3rj3)

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