



# CVE-2023-38877

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2023-38877                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | cve@mitre.org                                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2023-09-28 04:15:00 UTC                                                                                                   |
| <b>Updated</b>         | 2023-10-02 18:45:00 UTC                                                                                                   |
| <b>Description</b>     | A host header injection vulnerability exists in gugoan's Economizzer v.0.9-beta1 and commit 3730880 (April 2023). By send |

## Risk And Classification

### Problem Types: CWE-94

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                      | Product                     | Version    | Update | Edition | Language |
|-------------|-----------------------------|-----------------------------|------------|--------|---------|----------|
| Application | <a href="#">Economizzer</a> | <a href="#">Economizzer</a> | 0.9        | beta1  | All     | All      |
| Application | <a href="#">Economizzer</a> | <a href="#">Economizzer</a> | april_2023 | All    | All     | All      |

## References

| Reference                                                                        | Source  | Link                                | Tags           |
|----------------------------------------------------------------------------------|---------|-------------------------------------|----------------|
| GitHub - gugoan/economizzer: Open Source Personal Finance Manager                | MISC    | <a href="#">github.com</a>          |                |
| Economizzer - Open Source Personal Finance Manager                               | MISC    | <a href="#">www.economizzer.org</a> |                |
| CVE-2023-38877: Host Header Injection in Forgot Password of gugoan's Economizzer | MISC    | <a href="#">github.com</a>          |                |
| CVE Program record                                                               | CVE.ORG | <a href="#">www.cve.org</a>         | canonical      |
| NVD vulnerability detail                                                         | NVD     | <a href="#">nvd.nist.gov</a>        | canonical, ana |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[995451](#) PHP (Composer) Security Update for gugoan/economizzer (GHSA-hqp9-mrjw-7qq2)

© [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](#)