



CVE-2023-37260

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-37260
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-06 16:15:00 UTC
Updated	2023-07-13 19:25:00 UTC
Description	league/oauth2-server is an implementation of an OAuth 2.0 authorization server written in PHP. Starting in version 8.3.2 an

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thephleague	Oauth2-server	All	All	All	All

References

Reference

- [Remove Key Leak by Sephster · Pull Request #1353 · thephleague/oauth2-server · GitHub](#)
- [Key exposed in exception message when passing as a string and providing an invalid pass phrase · Advisory · thephleague/oauth2-server · CVE](#)
- [Release 8.5.3 · thephleague/oauth2-server · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

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