



CVE-2023-38759

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

Summary

CVE	CVE-2023-38759
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-08 16:15:00 UTC
Updated	2023-08-11 16:06:00 UTC
Description	Cross Site Request Forgery (CSRF) vulnerability in wger Project wger Workout Manager 2.2.0a3 allows a remote attacker t

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wger	Workout Manager	2.2.0	a3	All	All

References

Reference	Source	Link	Tags
GitHub - 0x72303074/CVE-Disclosures	MISC	github.com	
wger Workout Manager - Features	MISC	wger.de	
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

[994908](#) Python (Pip) Security Update for wger (GHSA-wrw3-qmqw-4x9w)

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