



CVE-2023-23710

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

Summary

CVE	CVE-2023-23710
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-25 20:15:00 UTC
Updated	2023-04-28 19:26:00 UTC
Description	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in miniOrange WordPress Social Login and Register (Discor

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Wordpress Social Login And Register Discord Google Twitter LinkedIn	All	All	All	All

References

Reference

- WordPress WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin <= 7.5.14 - Cross Site Scripting (XSS) vulnerability
- 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.

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