CVE-2022-34149

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-34149
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-22 15:15:00 UTC
Updated	2023-04-20 09:15:00 UTC
Description	Authentication Bypass vulnerability in miniOrange WP OAuth Server plugin <= 3.0.4 at WordPress.

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Wp Oauth Server	All	All	All	All

References

Reference	Source	Link
WP OAuth Server (Login with WordPress) – WordPress plugin | WordPress.org	CONFIRM	wordpress.c
WordPress WP OAuth Server plugin <= 3.0.4 - Authentication Bypass vulnerability - Patchstack	CONFIRM	patchstack.c
WordPress WP OAuth Server plugin <= 3.0.4 - Authentication Bypass vulnerability - Patchstack	MISC	patchstack.c
WP OAuth Server (Login with WordPress) by miniOrange WordPress plugin Authentication Bypass – Lana Codes	MISC	lana.codes
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report