



CVE-2022-34858

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

Summary

CVE	CVE-2022-34858
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-22 15:15:00 UTC
Updated	2023-08-02 17:20:00 UTC
Description	Authentication Bypass vulnerability in miniOrange OAuth 2.0 client for SSO plugin <= 1.11.3 at WordPress.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Oauth 2.0 Client For Sso	All	All	All	All

References

Reference	Source	Link	Tag
WordPress OAuth 2.0 client for SSO plugin <= 1.11.3 - Authentication Bypass vulnerability - Patchstack	CONFIRM	patchstack.com	
WordPress OAuth 2.0 client for SSO plugin <= 1.11.3 - Authentication Bypass vulnerability - Patchstack	MISC	patchstack.com	
OAuth 2.0 client for SSO by miniOrange WordPress plugin Authentication Bypass – Lana Codes	MISC	lana.codes	
OAuth 2.0 client for SSO – WordPress plugin WordPress.org	CONFIRM	wordpress.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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