CVE-2022-2083

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

Summary

CVE	CVE-2022-2083
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-05 13:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	The Simple Single Sign On WordPress plugin through 4.1.0 leaks its OAuth client_secret, which could be used by attackers

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple Sign On Project	Simple Sign On	All	All	All	All

References

Reference	Source	Link	Tags
Simple Single Sign On by Dash10 Digital WordPress plugin Authentication Bypass – Lana Codes	MISC	lana.codes	
Simple Single Sign On <= 4.1.0 - Authentication Bypass WordPress Security Vulnerability	MISC	wpscan.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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**