CVE-2022-4496

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

Summary

CVE	CVE-2022-4496
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-30 21:15:00 UTC
Updated	2023-11-07 03:57:00 UTC
Description	The SAML SSO Standard WordPress plugin version 16.0.0 before 16.0.8, SAML SSO Premium WordPress plugin version

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniorange	Saml Sp Single Sign On	All	All	All	All
Application	Miniorange	Saml Sp Single Sign On	All	All	All	All
Application	Miniorange	Saml Sp Single Sign On	All	All	All	All

References

Reference	Source
miniOrange WordPress SAML SSO Premium < 12.1.0 - Open Redirect in SSO login WordPress Security Vulnerability	MISC
miniOrange WordPress SAML SSO Standard < 16.0.8 - Open Redirect in SSO login WordPress Security Vulnerability	MISC
miniOrange WordPress SAML SSO Premium Multisite < 20.0.7 - Open Redirect in SSO login WordPress Security Vulnerability	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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**