CVE-2019-12346

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-12346
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-24 21:15:00 UTC
Updated	2019-06-27 11:15:00 UTC
Description	In the miniOrange SAML SP Single Sign On plugin before 4.8.73 for WordPress, the SAML Login Endpoint is vulnerable to

Risk And Classification

Problem Types: CWE-79

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

References

Reference	Source	Link	Tags
SAML SP Single Sign On <= 4.8.72 - Cross-Site Scripting (XSS)	MISC	wpvulndb.com	
CVE-2019-12346 – miniOrange SAML SP Single Sign On WordPress Plugin XSS – ZeroAuth	MISC	zeroauth.ltd	Exploit, Third P
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

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