



CVE-2020-14445

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

Summary

CVE	CVE-2020-14445
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-18 18:15:00 UTC
Updated	2022-11-16 03:57:00 UTC
Description	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential F

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wso2	Identity Server	All	All	All	All
Application	Wso2	Identity Server As Key Manager	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-14445 - Stored Cross-Site Scripting (XSS) in WSO2 Product	MISC	cybersecurityworks.com	
Security Advisory WSO2-2020-0711 - WSO2 Platform Security - WSO2 Documentation	CONFIRM	docs.wso2.com	Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

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