



CVE-2019-5729

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

Summary

CVE	CVE-2019-5729
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2019-03-27 13:54:00 UTC
Description	Splunk-SDK-Python before 1.6.6 does not properly verify untrusted TLS server certificates, which could result in man-in-the

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Software Development Kit	All	All	All	All
Application	Splunk	Software Development Kit	All	All	All	All

References

Reference	Source	Link	Tags
SP-CAAQAD Splunk	CONFIRM	www.splunk.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981116 Python (pip) Security Update for splunk-sdk (GHSA-f58w-649r-qjr9)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)