



CVE-2017-6667

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

Summary

CVE	CVE-2017-6667
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-13 06:29:00 UTC
Updated	2017-06-26 14:54:00 UTC
Description	A vulnerability in the update process for the dynamic JAR file of the Cisco Context Service software development kit (SDK)

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Context Service Development Kit	2.0	All	All	All
Application	Cisco	Context Service Development Kit	2.0	All	All	All

References

Reference	Source	Link	Tags
Cisco Context Service SDK Arbitrary Code Execution Vulnerability	CONFIRM	tools.cisco.com	Vendor Advisory
Cisco Context Service SDK CVE-2017-6667 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

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