



CVE-2017-5643

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

Summary

CVE	CVE-2017-5643
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-16 15:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	Apache Camel's Validation Component is vulnerable against SSRF via remote DTDs and XXE.

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Camel	2.17.0	All	All	All
Application	Apache	Camel	2.17.1	All	All	All
Application	Apache	Camel	2.17.2	All	All	All
Application	Apache	Camel	2.17.3	All	All	All
Application	Apache	Camel	2.17.4	All	All	All
Application	Apache	Camel	2.17.5	All	All	All
Application	Apache	Camel	2.18.0	All	All	All
Application	Apache	Camel	2.18.1	All	All	All
Application	Apache	Camel	2.18.2	All	All	All
Application	Apache	Camel	2.17.0	All	All	All
Application	Apache	Camel	2.17.1	All	All	All
Application	Apache	Camel	2.17.2	All	All	All
Application	Apache	Camel	2.17.3	All	All	All
Application	Apache	Camel	2.17.4	All	All	All
Application	Apache	Camel	2.17.5	All	All	All
Application	Apache	Camel	2.18.0	All	All	All
Application	Apache	Camel	2.18.1	All	All	All

Application	Apache	Camel	2.18.2	All	All	All
Application	Apache	Camel	All	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	Mailing L
Pony Mail!		lists.apache.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Pa
camel.apache.org/security-advisories.data/CVE-2017-5643.txt.asc	CONFIRM	camel.apache.org	Vendor /
Apache Camel CVE-2017-5643 Server Side Request Forgery Security Bypass Vulnerability	BID	www.securityfocus.com	Third Pa
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980840 Java (maven) Security Update for org.apache.camel:camel-core (GHSA-vq9j-jh62-5hmp)