



CVE-2022-25167

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-25167
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-14 08:15:00 UTC
Updated	2022-06-27 16:42:00 UTC
Description	Apache Flume versions 1.4.0 through 1.9.0 are vulnerable to a remote code execution (RCE) attack when a configuration u

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Flume	All	All	All	All

References

Reference	Source	Link	T
N/A	CONFIRM	lists.apache.org	
[FLUME-3416] Improve input validation in JMSSource - ASF JIRA	CONFIRM	issues.apache.org	
oss-security - CVE-2022-25167 - Apache Flume JMSSource does not protect from malicious JNDI urls	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376702](#) Apache Flume JNDI Remote Code Execution (RCE) Vulnerability in JMSSource

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

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