



CVE-2019-0187

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

Summary

CVE	CVE-2019-0187
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-06 17:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Unauthenticated RCE is possible when JMeter is used in distributed mode (-r or -R command line options). Attacker can es

Risk And Classification

Problem Types: CWE-327 | CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Jmeter	4.0	All	All	All
Application	Apache	Jmeter	5.0	All	All	All
Application	Apache	Jmeter	4.0	All	All	All
Application	Apache	Jmeter	5.0	All	All	All

References

Reference	Source	Link
Apache JMeter CVE-2019-0187 Remote Code Execution Vulnerability	BID	www.securiti
[SECURITY] CVE-2019-0187: Apache JMeter Missing client auth for RMI connection when distributed test is used	MLIST	mail-archive
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980811](#) Java (maven) Security Update for org.apache.jmeter:ApacheJMeter (GHSA-wg37-7mrv-cfwm)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

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