



Apache OpenMeetings: Login Credentials Passed via GET Query Parameters

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

Summary

CVE	CVE-2026-34020
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 16:16:27 UTC
Updated	2026-04-09 17:16:25 UTC
Description	Use of GET Request Method With Sensitive Query Strings vulnerability in Apache OpenMeetings. The REST login endpoint

Risk And Classification

Problem Types: CWE-598 | CWE-598 CWE-598 Use of GET Request Method With Sensitive Query Strings

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache OpenMeetings	affected 3.1.3 9.0.0 semver	Not specified

References

Reference	Source	Link
owasp.org/www-community/vulnerabilities/Information_exposure_through_qu...	security@apache.org	owasp.org
lists.apache.org/thread/2h3h9do5tp17xldr0nps1yjmkx4vs3db	security@apache.org	lists.apache.org
www.openwall.com/lists/oss-security/2026/04/09/12	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: 4ra2n (A code security AI agent) (en)

There are currently no legacy QID mappings associated with this CVE.

© [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](#)