



CVE-2023-44981

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

Summary

CVE	CVE-2023-44981
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-11 12:15:00 UTC
Updated	2023-11-01 07:15:00 UTC
Description	Authorization Bypass Through User-Controlled Key vulnerability in Apache ZooKeeper. If SASL Quorum Peer authentication

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Zookeeper	All	All	All	All
Application	Apache	Zookeeper	3.9.0	All	All	All

References

Reference	Source	Link
oss-security - CVE-2023-44981: Apache ZooKeeper: Authorization bypass in SASL Quorum Peer Authentication	MISC	www.openwa
lists.apache.org/thread/wf0yrk84dg1942z1o74kd8nycg6pgm5b	MISC	lists.apache.c
Debian -- Security Information -- DSA-5544-1 zookeeper	MISC	www.debian.o
[SECURITY] [DLA 3624-1] zookeeper security update	MISC	lists.debian.o
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[200055](#) Ubuntu Security Notification for ZooKeeper Vulnerabilities (USN-6559-1)

[6000252](#) Debian Security Update for zookeeper (DLA 3624-1)

6000311 Debian Security Update for zookeeper (DSA 5544-1)

691372 Free Berkeley Software Distribution (FreeBSD) Security Update for apache (2bc376c0-977e-11ee-b4bc-b42e991fc52e)

995568 Java (Maven) Security Update for org.apache.zookeeper:zookeeper (GHSA-7286-pgfv-vxvh)

© [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](#).

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