



CVE-2020-35451

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

Summary

CVE	CVE-2020-35451
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-09 16:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	There is a race condition in OozieSharelibCLI in Apache Oozie before version 5.2.1 which allows a malicious attacker to re

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
oss-security - CVE-2020-35451: Oozie local privilege escalation	MLIST	www.openwall.com	Mailing List, Third Party Advisory
Pony Mail!	MISC	lists.apache.org	Mailing List, Vendor Advisory
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: The Apache Oozie PMC would like to thank Jonathan Leitschuh for reporting the issue

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](#)