



CVE-2020-13929

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

Summary

CVE	CVE-2020-13929
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-02 17:15:00 UTC
Updated	2023-11-24 14:15:00 UTC
Description	Authentication bypass vulnerability in Apache Zeppelin allows an attacker to bypass Zeppelin authentication mechanism to

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
[zeppelin-users] 20210928 Re: CVE-2020-13929: Apache Zeppelin: Notebook permissions bypass		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MISC	lists.apache.org	
oss-security - CVE-2020-13929: Apache Zeppelin: Notebook permissions bypass	MLIST	www.openwall.com	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Zeppelin: Multiple Vulnerabilities (GLSA 202311-04) — Gentoo security		security.gentoo.org	
Pony Mail!	MLIST	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Zeppelin would like to thank David Woodhouse for reporting this issue

Legacy QID Mappings	
710787	Gentoo Linux Zeppelin Multiple Vulnerabilities (GLSA 202311-04)
730205	Apache Zeppelin Multiple Vulnerabilities
980636	Java (maven) Security Update for org.apache.zeppelin:zeppelin (GHSA-87p2-cvhq-q4mv)

© [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](#)