



CVE-2021-27578

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

Summary

CVE	CVE-2021-27578
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	Cross Site Scripting vulnerability in markdown interpreter of Apache Zeppelin allows an attacker to inject malicious scripts.

Risk And Classification

Problem Types: CWE-79

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
Pony Mail!	MLIST	lists.apache.org
[announce] 20210902 CVE-2021-27578: Apache Zeppelin: Cross Site Scripting in markdown interpreter		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
[zeppelin-users] 20210928 Re: CVE-2021-27578: Apache Zeppelin: Cross Site Scripting in markdown interpreter		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
oss-security - CVE-2021-27578: Apache Zeppelin: Cross Site Scripting in markdown interpreter	MLIST	www.openwall.com
Zeppelin: Multiple Vulnerabilities (GLSA 202311-04) — Gentoo security		security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Zeppelin would like to thank Paulo Pacheco for reporting this issue

Legacy QID Mappings	
710787	Gentoo Linux Zeppelin Multiple Vulnerabilities (GLSA 202311-04)
730205	Apache Zeppelin Multiple Vulnerabilities
980639	Java (maven) Security Update for org.apache.zeppelin:zeppelin (GHSA-mf7q-gw5f-q8jj)

© [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](#)