



CVE-2021-20727

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

Summary

CVE	CVE-2021-20727
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-27 09:15:00 UTC
Updated	2021-06-01 21:31:00 UTC
Description	Cross-site scripting vulnerability in Zettlr from 0.20.0 to 1.8.8 allows an attacker to execute an arbitrary script by loading a fil

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zettlr	Zettlr	All	All	All	All

References

Reference	Source	Link	Tags
A Markdown Editor for the 21st Century Zettlr	MISC	www.zettlr.com	
GitHub - Zettlr/Zettlr: A Markdown Editor for the 21st century.	MISC	github.com	
JVN#98239374: Zettlr vulnerable to cross-site scripting	MISC	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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