New issue

Jump to bottom

Security Issue: CSRF in DeleteFile function. [bug] #64

Closed **lethanhtrung222** opened this issue on Apr 19, 2020 · 5 comments

Labels security

lethanhtrung222 commented on Apr 19, 2020

```
In the source code, the DeleteFile function  is sent via unauthenticated GET method. (fp-plugins\mediamanager\tpls\admin.plugin.mediamanager.files.tpl
                <td>
                        <a class="link-delete" href="{$mmbaseurl}&deletefile={$v.type}-{$v.name}">{$plang.delete}</a>
                </td>
The application does not have anti-csrf tokens, so it is vulnerable to Cross-site Request Forgery attacks. The vulnerability allows delete any file.
```

lethanhtrung222 changed the title ~~Security Issue: CSRF in DeleteFile function.~~ **Security Issue: CSRF in DeleteFile function. [bug]** on Apr 19, 2020

lethanhtrung222 commented on Apr 19, 2020 Author

Similar to the file deletion feature, the post deletion feature and the plugins off feature, I also discovered the CSRF bug.

I can delete any entry and disable any plugins.

lethanhtrung222 commented on Apr 19, 2020 Author

Your endpoint:
/flat/admin.php?p=entry&action=delete&entry=
/flat/admin.php?p=plugin&action=default&disableantispam&_wpnonce=
/flat/admin.php?p=uploader&action=mediamanager&deletefile=
/flat/admin.php?p=uploader&action=mediamanager&deletefile=gallery-

azett added the security label on Apr 19, 2020

azett commented on Apr 21, 2020 • edited Member

Confirmed, thank you very much for finding and reporting this!

I branched v1.1 to "issue64", so we can publish a bugfix release 1.1.1 as soon as the problem is solved.

azett added a commit that referenced this issue on Oct 18, 2020

`Introduced a session token to prevent possible CSRF attacks. See #64,…` ... `bb10fd7`

azett commented on Oct 18, 2020 Member

Fixed with `bb10fd7` in Branch issue64. Thank you very much for reporting!

azett closed this as completed on Oct 18, 2020

lethanhtrung222 commented on Oct 19, 2020 Author

Thank you.

Vào CN, 18 thg 10, 2020 vào lúc 04:29 Arvid Zimmermann <
notifications@github.com> đã viết:
...

Assignees
No one assigned

Labels
security

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants