

# FileImporter allows imports to cascade protected files when the importer does not have administrator permissions (CVE-2022-28206)

[Actions](#)☒ Closed, Resolved Public

3 Estimated Story Points

SECURITY

## Assigned To


WMDE-Fisch

## Authored By

Dylsss

2021-10-25 14:59:23 (UTC+0)

## Tags

 Security-Team (Our Part Is Done) Security Move-Files-To-Commons (Backlog) WMDE-TechWish (Proposed) WMDE-TechWish-Maintenance (In progress) WMDE-TechWish-Sprint-2022-01-19 (Done) SecTeam-Processed (Completed) Vuln-MissingAuthz (Tracked)

## Referenced Files

**F34930634: Screenshot 2022-01-25 205553.jpg**

2022-01-25 20:56:52 (UTC+0)

## Subscribers

Aklapper

Andrew-WMDE

awight

Dylsss

Lena\_WMDE

lilients\_WMDE

sbassett

[View All 9 Subscribers](#)

## Description

### Steps to reproduce

- Protect a page with cascading turned on
- Transclude a non-existent file onto it
- Import a file to the title which is now cascade protected, using an account without administrator permissions

The import completes successfully, bypassing the cascade protection and creating the page. Similar to **T262628**.

## Details

### Risk Rating

Low

### Author Affiliation

Wikimedia Communities

#### Project

#### Subject



[mediawiki/extensions/FileImporter](#)

[Check edit rights before uploading](#)

[Customize query in Gerrit](#)

## Related Objects

### Mentions

#### Mentioned In

~~T297839: Write and send supplementary release announcement for extensions and skins with security patches (1.35.6/1.36.4/1.37.2)~~


#### Mentioned Here


~~T297839: Write and send supplementary release announcement for extensions and skins with security patches (1.35.6/1.36.4/1.37.2)~~

~~T262628: FileImporter imports the file even when the target page is protected on Commons and the importer should not be able to create it (CVE-2020-26121)~~

- Dylsss** created this task. 2021-10-25 14:59:23 (UTC+0)
- Restricted Application added a subscriber: **Aklapper**. · [View Herald Transcript](#) 2021-10-25 14:59:25 (UTC+0)
- Dylsss** renamed this task from *FileImporter allows imports to cascade protected files when the importer does not have administartor permissions* to *FileImporter allows imports to cascade protected files when the importer does not have administrator permissions*. 2021-10-25 15:00:13 (UTC+0)
- Dylsss** added a project: **Move-Files-To-Commons**.
- Dylsss** updated the task description. (**Show Details**) 2021-10-25 15:03:27 (UTC+0)

 **Reedy** added projects: **WMDE-TechWish**, **WMDE-TechWish-Maintenance**. 2021-10-25 15:48:28 (UTC+0)


 **Reedy** moved this task from **Incoming** to **Watching** on the **Security-Team** board.

 **Dylsss** added a comment. 2022-01-06 23:28:19 (UTC+0)

The issue appears to be that FileImporter only does checks for create and upload, but not edit. This results in no errors being returned because the `PermissionManager::checkCascadingSourcesRestrictions` check directly compares the given action to the cascading action restriction (which is only ever edit), this means any checks for actions other than edit will never return errors for cascading restrictions. It looks like the abandoned patch <https:// Gerrit.wikimedia.org/r/c/mediawiki/core/+233207> would have addressed this bug.


 **thiemowmde** added subscribers: **Lena\_WMDE**, **lilients\_WMDE**, **awight** and **3 others**. 2022-01-07 08:55:16 (UTC+0)

 **thiemowmde** moved this task from **Incoming** to **Priority backlog** on the **WMDE-TechWish-Maintenance** board.  
2022-01-18 13:34:49 (UTC+0)

 **WMDE-Fisch** claimed this task. 2022-01-25 14:37:56 (UTC+0)

 **WMDE-Fisch** added a project: **WMDE-TechWish-Sprint-2022-01-19**.

 **WMDE-Fisch** moved this task from **Sprint Backlog** to **Doing** on the **WMDE-TechWish-Sprint-2022-01-19** board.

 **WMDE-Fisch** added a comment. 2022-01-25 16:07:38 (UTC+0)

In **T294256#7603240**, **@Dylsss** wrote:

*The issue appears to be that FileImporter only does checks for create and upload, but not edit. This results in no errors being returned because the `PermissionManager::checkCascadingSourcesRestrictions` check directly compares the given action to the cascading action restriction (which is only ever edit), this means any checks for actions other than edit will never return errors for cascading restrictions. It looks like the abandoned patch <https:// Gerrit.wikimedia.org/r/c/mediawiki/core/+233207> would have addressed this bug.*

I tried to solve the issue by adding a check for edit permissions. But from my local smoke tests it did not seem to work. Maybe I misunderstood the comment, and this would only work anyways with the other patch mentioned. 🤔  
See <https:// Gerrit.wikimedia.org/r/c/mediawiki/extensions/FileImporter/+757022>

What I did to test:

- Transcluded a non existing file page ( `{{File:Test.jpg}}` ) into a page ( `Main Page` ) on my wiki.
- Used an admin account to cascade protect `Main Page` and only allow changes for admins.
- Used a normal user account with the `FileImporter` to import a random `.jpg` file and use the name `Test` for the import.
- There should be an error on the import preview page but there's nothing.

I also tried to just upload a file with that name as a normal user and that also worked although the file page should be cascade protected.

👤 **WMDE-Fisch** removed **WMDE-Fisch** as the assignee of this task. 2022-01-25 16:08:29 (UTC+0)

📋 **WMDE-Fisch** moved this task from **Doing** to **Sprint Backlog** on the ~~**WMDE-TechWish-Sprint-2022-01-19**~~ board.

📋 **WMDE-Fisch** moved this task from **Priority backlog** to **In progress** on the **WMDE-TechWish-Maintenance** board.

💬 **Dylsss** added a comment. 2022-01-25 20:56:52 (UTC+0)

@WMDE-Fisch Your patch works locally for me?



📋 **WMDE-Fisch** moved this task from **Sprint Backlog** to **Tech Review** on the ~~**WMDE-TechWish-Sprint-2022-01-19**~~ board. 2022-01-26 13:53:30 (UTC+0)

💬 **WMDE-Fisch** added a comment. 2022-01-28 15:13:58 (UTC+0)

In ~~**T294256#7650447**~~, @Dylsss wrote:

@WMDE-Fisch Your patch works locally for me?



Thanks for testing, still have not figured out, why I can not test it locally. We might just merge the patch and test it on the beta cluster before train rollout.

💬 **Dylsss** added a comment. 2022-01-28 19:42:15 (UTC+0)

@WMDE-Fisch I looked over your comment again, and I think it's not working because you are transcluding it like `{{File:Test.jpg}}` instead of `[[File:Test.jpg]]`. The former doesn't get any cascading protection.

💬 **WMDE-Fisch** added a comment. 2022-01-31 09:18:02 (UTC+0)


In ~~**T294256#7660456**~~, @Dylsss wrote:


@WMDE-Fisch I looked over your comment again, and I think it's not working because you are transcluding it like `{{File:Test.jpg}}` instead of `[[File:Test.jpg]]`. The former doesn't get any cascading protection.

 thanks for looking at it again and the clarification. Now I could confirm it working as well. Nice!

 **thiemowmde** assigned this task to **WMDE-Fisch**. 2022-01-31 09:42:21 (UTC+0)

 **thiemowmde** moved this task from **Tech Review** to **Demo** on the ~~**WMDE-TechWish-Sprint-2022-01-19**~~ board.

 **WMDE-Fisch** set the point value for this task to 3. 2022-01-31 13:29:13 (UTC+0)


 **thiemowmde** closed this task as *Resolved*. 2022-02-01 09:35:50 (UTC+0)

 **thiemowmde** moved this task from **Demo** to **Done** on the ~~**WMDE-TechWish-Sprint-2022-01-19**~~ board.

 **sbassett** mentioned this in ~~**T297839: Write and send supplementary release announcement for extensions and skins with security patches (1.35.6/1.36.4/1.37.2)**~~. 2022-02-01 15:47:45 (UTC+0)


 **sbassett** added a subscriber: **sbassett**. 2022-02-01 15:50:48 (UTC+0) ▼

Eh, well, I guess this went through gerrit: <https://gerrit.wikimedia.org/r/c/mediawiki/extensions/FileImporter/+/757022>.  
I'll track it for the next supplemental release (**T297839**) and we can make the bug public once wmf.20 is done rolling out this week.


 **sbassett** moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board.  
2022-02-01 15:51:16 (UTC+0)

 **sbassett** added a project: **SecTeam-Processed**.

 **sbassett** added a project: **Vuln-MissingAuthz**. 2022-03-29 01:24:26 (UTC+0)

 **sbassett** renamed this task from *FileImporter allows imports to cascade protected files when the importer does not have administrator permissions* to *FileImporter allows imports to cascade protected files when the importer does not have administrator permissions (CVE-2022-28206)*. 2022-03-30 19:20:16 (UTC+0)

➔ **sbassett** triaged this task as *Low* priority. 2022-03-31 17:42:21 (UTC+0)

 **sbassett** changed Author Affiliation from N/A to Wikimedia Communities.

 **sbassett** changed the visibility from "**Custom Policy**" to "Public (No Login Required)".

 **sbassett** changed the edit policy from "**Custom Policy**" to "All Users".

 **sbassett** changed Risk Rating from N/A to Low.