Special:ImportFile does not check permissions from own config FileImporterRequiredRight (CVE-2021-36132)

Closed, Resolved   Public   2 Estimated Story Points   SECURITY

Actions

Assigned To

thiemowmde

Authored By

Umherirrender
2021-04-19 19:59:07 (UTC+0)

Tags

Security-Team (Our Part Is Done)
Security
Move-Files-To-Commons (Tickets in sprint)
WMDE-TechWish-Sprint-2021-04-28 (Done)
Unplanned-Sprint-Work
MW-1.37-notes (1.37.0-wmf.4; 2021-05-04)
Patch-For-Review

Referenced Files

None

Subscribers

Aklapper

Andrew-WMDE

awight

Lena_WMDE

lilients_WMDE

RhinosF1

sbassett

View All 11 Subscribers

Description

The FileImporter extension provides a `Special:ImportFile` and allows to set the needed rights for the special page with config `FileImporterRequiredRight`

Setting `$wgFileImporterRequiredRight = 'editinterface';` in LocalSettings.php does not shows a permission error on the special page when logged in as non-sysop.
Without `$wgFileImporterShowInputScreen = true;` is does not give a input form, but it handles actions given by request params.

The function `SpecialPage::userCanExecute` is not executed on the special page. The `SpecialPage::__constructor` mention to call it itself when override execute, which is not happen here.
The permission is only taken into account on `Special:SpecialPages` and the page is not listed there.
It needs a call to `SpecialPage::checkPermissions` to handle the user right from the option.

I have not tested if one of the action of that special page could be executed without the necessary rights, I have only seen that the permission error is missing when first open the page.

The special page correctly checks if the upload is enabled on the wiki and the default permission is `upload`. In the default config there is no security issue, because `UploadBase::isAllowed` already checks for the upload right. Only when using customized the needed rights it is executed.

Maybe there is no need for such a option and the option needs to be removed without further mention of the security issue.

wmf wikis does not change or use the config.

Details

	Project	Subject
ᚹ	mediawiki/extensions/FileImporter	Fix incomplete check for $wgFileImporterRequiredRight
ᚹ	mediawiki/extensions/FileImporter	Fix incomplete check for $wgFileImporterRequiredRight
ᚹ	mediawiki/extensions/FileImporter	Fix incomplete check for $wgFileImporterRequiredRight

Customize query in gerrit

Related Objects

Mentions

Mentioned In

~~T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)~~

Umherirrender created this task. 2021-04-19 19:59:07 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-04-19 19:59:08 (UTC+0)

sbassett added a project: **Move-Files-To-Commons**. 2021-04-19 20:32:07 (UTC+0)

sbassett added subscribers: **thiemowmde**, **Urbanecm**.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2021-04-26 15:08:39 (UTC+0)

sbassett added a subscriber: **sbassett**. Edited · 2021-04-26 20:27:30 (UTC+0)

This appears to be a legitimate issue, if I'm understanding the permissions model correctly. It was probably never noticed on the projects since `$wgFileImporterRequiredRight` defaults to `upload` and every non-anon user has that right. I just tested with a brand new account on commons and when I navigated to:

https://commons.wikimedia.org/wiki/Special:ImportFile

I didn't see the form, but when I navigated to:

https://commons.wikimedia.org/wiki/Special:ImportFile?clientUrl=https://test.wikipedia.org/wiki/File:SD0002test.png

I could view the import form and was able to import another example to commons (e.g. this image). This all makes sense since every non-anon has `edit` and `upload`. The relevant code for `UploadBase::isAllowed` hasn't changed in a long time, so I suppose `SpecialImportFile::executeStandardChecks` should be checking `$wgFileImporterRequiredRight` around here for this to be properly implemented. Maybe something like:

```
$permissionRequired = UploadBase::isAllowed( $user ) &&
    $user->isAllowed( $this->config->get( 'FileImporterRequiredRight' ) );
```

sbassett mentioned this in ~~T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)~~. 2021-04-27 18:06:44 (UTC+0)

thiemowmde claimed this task. 2021-04-30 12:39:32 (UTC+0)

thiemowmde set the point value for this task to *2*.

thiemowmde moved this task from **Backlog** to **Tickets in sprint** on the **Move-Files-To-Commons** board.

thiemowmde added projects: ~~**WMDE-TechWish-Sprint-2021-04-28**~~, **Unplanned-Sprint-Work**.

thiemowmde added subscribers: **Lena_WMDE**, **WMDE-Fisch**.

thiemowmde added a project: **Patch-For-Review**. 2021-04-30 12:47:49 (UTC+0)

thiemowmde added subscribers: **Andrew-WMDE**, **lilients_WMDE**, **awight**.

As written at https://gerrit.wikimedia.org/r/c/mediawiki/extensions/FileImporter/+/683860 this is not relevant on the Wikimedia cluster. The `$wgFileImporterRequiredRight` config is set to "upload" by default, but the upload right is checked anyway, independent from that config. The config was introduced for 2 reasons:

- To be able to quickly change it in case there is a legitimate reason to limit the user group allowed to use the special page.
- For 3rd party installations.

While this is a legitimate bug, it does not allow to bypass the upload restriction. Therefor I think this does not need to be market as a restricted security issue.

thiemowmde moved this task from **Sprint Backlog** to **Review** on the ~~**WMDE-TechWish-Sprint-2021-04-28**~~ board. 2021-04-30 12:55:13 (UTC+0)

sbassett added a comment. 2021-04-30 14:25:23 (UTC+0)

> In ~~**T280590#7048819**~~, **@thiemowmde** wrote:
>
> *While this is a legitimate bug, it does not allow to bypass the upload restriction. Therefor I think this does not need to be market as a restricted security issue.*

That's a fair assessment, I'll make this task public now.

sbassett triaged this task as *Medium* priority. 2021-04-30 14:25:39 (UTC+0)

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

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

RhinosF1 added a subscriber: **RhinosF1**. 2021-04-30 15:16:55 (UTC+0)

thiemowmde moved this task from **Review** to **Demo** on the ~~**WMDE-TechWish-Sprint-2021-04-28**~~ board. 2021-05-03 07:39:22 (UTC+0)

gerritbot added a comment. 2021-05-03 07:45:28 (UTC+0)

Change 683860 **merged** by jenkins-bot:

[mediawiki/extensions/FileImporter@master] Fix incomplete check for $wgFileImporterRequiredRight

https://gerrit.wikimedia.org/r/683860

ReleaseTaggerBot added a project: ~~**MW-1.37-notes (1.37.0-wmf.4; 2021-05-04)**~~. 2021-05-03 08:00:29 (UTC+0)

sbassett moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board. 2021-05-03 14:06:32 (UTC+0)

sbassett removed a project: **Patch-For-Review**.

thiemowmde moved this task from **Demo** to **Done** on the ~~**WMDE-TechWish-Sprint-2021-04-28**~~ board. 2021-05-11 12:36:56 (UTC+0)

sbassett closed this task as *Resolved*. 2021-05-17 17:04:46 (UTC+0)

gerritbot added a comment. 2021-07-01 21:37:04 (UTC+0)

Change 702712 had a related patch set uploaded (by SBassett; author: Thiemo Kreuz (WMDE)):

[mediawiki/extensions/FileImporter@REL1_36] Fix incomplete check for $wgFileImporterRequiredRight

https://gerrit.wikimedia.org/r/702712

gerritbot added a project: **Patch-For-Review**. 2021-07-01 21:37:05 (UTC+0)

Change 702713 had a related patch set uploaded (by SBassett; author: Thiemo Kreuz (WMDE)):

[mediawiki/extensions/FileImporter@REL1_35] Fix incomplete check for $wgFileImporterRequiredRight

https://gerrit.wikimedia.org/r/702713

gerritbot added a comment. 2021-07-01 21:52:19 (UTC+0)

Change 702713 **merged** by jenkins-bot:

[mediawiki/extensions/FileImporter@REL1_35] Fix incomplete check for $wgFileImporterRequiredRight https://gerrit.wikimedia.org/r/702713

gerritbot added a comment. 2021-07-01 21:52:30 (UTC+0)

Change 702712 **merged** by jenkins-bot:

[mediawiki/extensions/FileImporter@REL1_36] Fix incomplete check for $wgFileImporterRequiredRight

https://gerrit.wikimedia.org/r/702712

sbassett renamed this task from *Special:ImportFile does not check permissions from own config FileImporterRequiredRight* to *Special:ImportFile does not check permissions from own config FileImporterRequiredRight (CVE-2021-36132)*.
2021-07-02 19:55:05 (UTC+0)