CVE-2021-30155: Titleblacklist didn't prevent creation of pages by Special:ChangeContentModel when a rule was met

Closed, Resolved · Public · SECURITY

Actions

Assigned To

taavi

Authored By

Xzonn
2021-01-01 09:37:08 (UTC+0)

Tags

TitleBlacklist (Backlog)
Security
Security-Team (Our Part Is Done)
MediaWiki-Page-editing (Backlog)
User-DannyS712 (Others)
User-Majavah (Done)
MW-1.31-release-notes
Vuln-Misconfiguration (Tracked)

Referenced Files

F34251706: 04-T270998-master.patch
2021-04-05 00:12:43 (UTC+0)

F34251707: 04-T270998-REL1_31.patch
2021-04-05 00:12:43 (UTC+0)

F34251705: 04-T270998-REL1_35.patch
2021-04-05 00:12:43 (UTC+0)

F33982707: T270988-PS3.patch
2021-01-02 09:00:05 (UTC+0)

F33981526: T270988-PS1.patch
2021-01-01 10:59:32 (UTC+0)

F33981528: T270988-PS2.patch
2021-01-01 10:59:32 (UTC+0)

Subscribers

Aklapper
DannyS712
gerritbot
Reedy
sbassett
taavi
Xzonn

Description

If a page does not exist, and someone just created it by `[[Special:ChangeContentModel]]`, even if it matched `[[MediaWiki:Titleblacklist]]`, it will still be created.

Eg. Add a line `.*` in `[[MediaWiki:Titleblacklist]]`, then let other user (who is not a sysop) open `[[Special:ChangeContentModel]]`, input any title, then change the model to whatever you like, then the page is created.

Steps to test: (all on testwiki)

1. Revoke `tboverride` from template editors (https://gerrit.wikimedia.org/r/654449/)
2. Add `User:DannyS712\/Bug.*` to title blacklist
3. Grant template editor rights to an alternate test account
4. Switch to using that alternate test account
5. Try to create `User:DannyS712/Bug 1` manually, to confirm its properly blacklisted
6. Try to create it via Special:ChangeContentModel, to confirm the bug exists
7. <deploy fix>
8. Try to create `User:DannyS712/Bug 2` via Special:ChangeContentModel, should fail

`includes/content/ContentModelChange.php` added in ~~**T107174: Add an API action to just change content model**~~ / **rMW0789d1568d76: Add a ContentModelChange helper, and an api module that uses it**

Details

	Project	Subject
P	mediawiki/core	SECURITY: ContentModelChange: Check that user can create pages

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

Status	Assigned	Task
Resolved	Reedy	~~T270458~~ Release MediaWiki 1.31.13/1.35.2

Resolved Reedy ~~T270459~~ **Tracking bug for MediaWiki 1.31.13/1.35.2**

Resolved taavi ~~T270988~~ **CVE-2021-30155: Titleblacklist didn't prevent creation of pages by Special:ChangeContentModel when a rule was met**

Xzonn created this task. 2021-01-01 09:37:08 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-01-01 09:37:08 (UTC+0)

taavi set Security to Software security bug. 2021-01-01 09:38:20 (UTC+0)

taavi added projects: **Security**, **Security-Team**.

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

taavi changed the subtype of this task from "Task" to "Security Issue".

taavi added a subscriber: **taavi**.

protecting as a security issue just in case

DannyS712 added projects: **MediaWiki-Page-editing**, **User-DannyS712**. Edited · 2021-01-01 09:49:10 (UTC+0)

DannyS712 added a subscriber: **DannyS712**.

`ContentModelChange` doesn't go through the normal edit page checks before creating the new revision, but rather uses `WikiPage::doEditContent` after implementing **some** checks. Since TitleBlacklistHooks::onUserCan and the subsequent code takes into account the action, and allows for disallowing page creation while allowing page edits, tweaking core's `ContentModelChange::checkPermissions` to also run checks for the `createpage` / `createtalk` action if the page doesn't already exist should allow TitleBlacklist to prevent the edit accordingly

Might be okay to post the patch publically on gerrit with an inconspicuous commit message, but something like replacing line 115 of the current code (https://gerrit.wikimedia.org/g/mediawiki/core/+/8ee4aa0df786d1216b02d49c3ae36bc468ef31a2/includes/content/ContentModelChange.php#115) with:

```
$creationErrors = [];
if ( !$current->exists() ) {
        $creationAction = $current->isTalkPage() ? 'createtalk' : 'createpage';
        $creationErrors = $pm->getPermissionErrors( $creationAction, $user, $current );
}
$errors = wfMergeErrorArrays(
        // Potentially include creation errors, if applicable
        $creationErrors,
```

I was about to log off when I saw this task, and wanted to document ^^^ and will try and see if that actually works to fix the issue soon

taavi added a comment. Edited · 2021-01-01 10:15:47 (UTC+0)

Danny's patch works for me with TitleBlacklist, I'll ~~add a test for that~~ and attach a patch file here shortly.

That's using `createpage` or `createtalk`, MediaWiki-extensions-ArticleCreationWorkflow looks to be using `create` [0], I'll also test if that is vulnerable.

[0] https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/extensions/ArticleCreationWorkflow/+/refs/heads/master/includes/Hooks.php#31

taavi added a comment. 2021-01-01 10:59:32 (UTC+0)

PS1, which is Danny's original fix in ~~**T270988#6715865**~~:

T270988-PS1.patch 1 KB
Download

PS2, including my change to also check for `create` action which some extensions use:

T270988-PS2.patch 1 KB
Download

I tried to add a test but failed with keeping the patch fairly small, I think that can be added after the fix publicly in Gerrit.

taavi added a project: **Patch-For-Review**. 2021-01-01 18:31:42 (UTC+0)

DannyS712 added a comment. 2021-01-01 23:39:13 (UTC+0)

> In ~~**T270988#6715890**~~, @Majavah wrote:
> *PS1, which is Danny's original fix in ~~**T270988#6715865**~~:*
>
> ***T270988-PS1.patch*** *1 KB*
> *Download*
>
> *PS2, including my change to also check for `create` action which some extensions use:*
>
> ***T270988-PS2.patch*** *1 KB*
> *Download*
>
> *I tried to add a test but failed with keeping the patch fairly small, I think that can be added after the fix publicly in Gerrit.*

Looking through the various Constraints in EditPage::internalAttemptSave

- ContentModelChangeConstraint checks if the user has `editcontentmodel` and can use it on the title with the new content model, as well as if they can `edit` the page with the new content model
- CreationPermissionConstraint checks if the user can `create` the page
- EditRightConstraint checks if the user can `edit` the page

So I don't think my original fix (or PS2) is ideal. Pretty sure it should **only** be checking `create` here, not `createpage` / `createtalk`

DannyS712 added a comment. 2021-01-02 08:26:07 (UTC+0)

See also **T271038: Use edit constraints within ContentModelChange**

taavi added a comment. 2021-01-02 09:00:05 (UTC+0)

PermissionManager will check for `createpage` / `createtalk` user rights when the action parameter is set to `create`. I don't think it checks for hooks modifying `createpage` / `createtalk` but all hooks I've seen do check for `create`, some also for `createpage` / `createtalk`.

PS3, only checking for `create`:

T270988-PS3.patch 1 KB
Download

DannyS712 added subscribers: **sbassett**, **Reedy**. 2021-01-02 09:33:54 (UTC+0)

PS3 - LGTM, CR+1, untested though. @sbassett @Reedy do you think that this can be done publically on gerrit with an inconspicuous commit message?

Reedy renamed this task from *Titleblacklist failed when creating pages by Special:ChangeContentModel* to *Titleblacklist didn't prevent creation of pages by Special:ChangeContentModel when a rule was met*. 2021-01-04 16:17:36 (UTC+0)

sbassett triaged this task as *Medium* priority. 2021-01-04 16:22:03 (UTC+0)

sbassett moved this task from **Incoming** to **In Progress** on the **Security-Team** board.

@DannyS712 - eh, let's be cautious and deploy this during the security window today. Would you or @Majavah be around at 22:00 UTC to help test? If not, I can probably manage the testing myself or just undeploy if anything bad happens.

taavi added a comment. 2021-01-04 16:24:31 (UTC+0)

@sbassett - Hi, unfortunately 22 UTC is midnight local time which is too late for me.

DannyS712 added a comment. 2021-01-05 00:24:25 (UTC+0)

> In ~~T270988#6719712~~, **@sbassett** wrote:
> *@DannyS712 - eh, let's be cautious and deploy this during the security window today. Would you or @Majavah be around at 22:00 UTC to help test? If not, I can probably manage the testing myself or just undeploy if anything bad happens.*

I should be able to be around at 22:00 UTC tomorrow (didn't see it for today) but we'll need to figure out how I can test this, since I don't know if there are wikis where I have admin rights to be able to set up the blacklist appropriately, **and** there is a local user group that has `editcontentmodel` but does not have `tboverride` (eg testwiki's template editors have both rights, as do enwikis)

sbassett added a comment. 2021-01-05 16:04:58 (UTC+0)

> In ~~T270988#6721467~~, **@DannyS712** wrote:
> *I should be able to be around at 22:00 UTC tomorrow*

Ok, let's try for that.

> *we'll need to figure out how I can test this, since I don't know if there are wikis where I have admin rights to be able to set up the blacklist appropriately*

testwiki? We're both sysops there and I can definitely edit MediaWiki:Titleblacklist to try some examples pre and post patch.

sbassett updated the task description. **(Show Details)** Edited · 2021-01-05 22:56:30 (UTC+0)

Failed to deploy today due to train issues, particularly **T271259**. Will try again tomorrow, 2021-01-06.

DannyS712 updated the task description. **(Show Details)** 2021-01-05 22:57:57 (UTC+0)

sbassett updated the task description. **(Show Details)** 2021-01-05 22:59:03 (UTC+0)

Aklapper added a comment. 2021-01-06 08:58:13 (UTC+0)

Hi, could you please use a common date format (which doesn't make an international audience think of First of June for a short moment)? Thanks a lot. :)

sbassett assigned this task to **taavi**. 2021-01-06 22:37:04 (UTC+0)

sbassett lowered the priority of this task from *Medium* to *Low*.

Deployed to .22 and .25 with @DannyS712's testing expertise. Let's hold this task/patch for the next security release (**T270458**).

Restricted Application added a project: ~~**User-Majavah**~~. · View Herald Transcript 2021-01-06 22:37:05 (UTC+0)

DannyS712 moved this task from **Unsorted** to **Others** on the **User-DannyS712** board. 2021-01-06 22:37:51 (UTC+0)

sbassett added a parent task: ~~**T270459: Tracking bug for MediaWiki 1.34.13/1.35.2**~~. 2021-01-06 22:40:12 (UTC+0)

sbassett removed a project: **Patch-For-Review**. 2021-01-07 17:23:00 (UTC+0)

taavi moved this task from **Unsorted** to **Done** on the ~~**User-Majavah**~~ board. 2021-01-23 20:31:48 (UTC+0)

Reedy mentioned this in ~~**T270459: Tracking bug for MediaWiki 1.34.13/1.35.2**~~. 2021-03-30 00:40:05 (UTC+0)

Reedy added a comment. 2021-04-04 22:40:53 (UTC+0)

Um... What happened to the patch for this? It doesn't seem to be deployed on WMF production, and the patch doesn't apply cleanly to master...

Reedy added a comment. 2021-04-04 23:32:50 (UTC+0)

Conflict is from **rMW932fbe24646d: Convert ContentModelChange to Authority**

Reedy updated the task description. **(Show Details)** 2021-04-04 23:36:11 (UTC+0)

Reedy added a comment. 2021-04-04 23:45:27 (UTC+0)

Patch as originally posted works fine on REL1_35.

For REL1_31, just needs moving back to includes/specials/SpecialChangeContentModel.php instead, and updates to use `getUserPermissionErrors`

```
commit 821b2250d57c2834b85ff31aeaa51df4edbf7024 (HEAD -> REL1_31)
Author: DannyS712 <dannys712.enwiki@gmail.com>
Date:   Fri Jan 1 12:40:41 2021 +0200

    SECURITY: ContentModelChange: Check that user can create pages

    Co-authored-by: Taavi Väänänen <hi@tassu.me>
    Change-Id: I2e3b79f36fa7c0a3ec4130de0ae9c68104cb3fdd

diff --git a/includes/specials/SpecialChangeContentModel.php b/includes/specials/SpecialChangeContentModel.php
index 87c899f4e0..8204dde46d 100644
--- a/includes/specials/SpecialChangeContentModel.php
+++ b/includes/specials/SpecialChangeContentModel.php
@@ -169,8 +169,16 @@ class SpecialChangeContentModel extends FormSpecialPage {
                $titleWithNewContentModel = clone $this->title;
                $titleWithNewContentModel->setContentModel( $data['model'] );
                $user = $this->getUser();
+
+               $creationErrors = [];
+               if ( !$current->exists() ) {
+                       $creationErrors = $this->title->getUserPermissionErrors( 'create', $user );
+               }
+
                // Check permissions and make sure the user has permission to:
                $errors = wfMergeErrorArrays(
+                       // Potentially include creation errors, if applicable
+                       $creationErrors,
                        // edit the contentmodel of the page
                        $this->title->getUserPermissionsErrors( 'editcontentmodel', $user ),
                        // edit the page under the old content model
```

Reedy added a comment. 2021-04-04 23:49:49 (UTC+0)

New patch for master

```
commit 180e0403774d535133c3b32d51ffa0fb4122df7b (HEAD -> master)
Author: DannyS712 <dannys712.enwiki@gmail.com>
Date:   Fri Jan 1 12:40:41 2021 +0200

    SECURITY: ContentModelChange: Check that user can create pages

    Co-authored-by: Taavi Väänänen <hi@tassu.me>
    Change-Id: I2e3b79f36fa7c0a3ec4130de0ae9c68104cb3fdd

diff --git a/includes/content/ContentModelChange.php b/includes/content/ContentModelChange.php
index 16a2ee520a..258bdf4953 100644
--- a/includes/content/ContentModelChange.php
+++ b/includes/content/ContentModelChange.php
@@ -113,6 +113,9 @@ class ContentModelChange {
                $titleWithNewContentModel->setContentModel( $this->newModel );

                $status = PermissionStatus::newEmpty();
+               if ( !$current->exists() ) {
+                       $authorizer( 'create', $current, $status );
+               }
                $authorizer( 'editcontentmodel', $current, $status );
                $authorizer( 'edit', $current, $status );
                $authorizer( 'editcontentmodel', $titleWithNewContentModel, $status );
```

Reedy added a comment. Edited · 2021-04-04 23:52:20 (UTC+0)

Which just leaves the question as to why it was undeployed from master... I'm guessing it's because of the conflict, maybe... But that really isnt' an acceptable reason.

It wasn't ever on the list on {T276237} either...

Reedy added a comment. 2021-04-05 00:12:43 (UTC+0)

04-T270998-REL1_31.patch 1 KB
Download

04-T270998-master.patch 1 KB
Download

04-T270998-REL1_35.patch 1 KB
Download

sbassett added a comment. 2021-04-05 20:51:17 (UTC+0)

Re-deployed master patch to wmf.37. Tracking again at T276237.

Reedy renamed this task from *Titleblacklist didn't prevent creation of pages by Special:ChangeContentModel when a rule was met* to *CVE-2021-30155: Titleblacklist didn't prevent creation of pages by Special:ChangeContentModel when a rule was met.* 2021-04-06 19:11:53 (UTC+0)

Reedy closed this task as *Resolved*. 2021-04-07 03:10:59 (UTC+0)

Reedy added a subscriber: **gerritbot**. 2021-04-08 19:11:29 (UTC+0)

gerritbot added a comment. 2021-04-08 19:53:10 (UTC+0)

Change 678040 had a related patch set uploaded (by Reedy; author: DannyS712):

[mediawiki/core@REL1_35] SECURITY: ContentModelChange: Check that user can create pages

https://gerrit.wikimedia.org/r/678040

gerritbot added a project: **Patch-For-Review**. 2021-04-08 19:53:13 (UTC+0)

gerritbot added a comment. 2021-04-08 20:18:20 (UTC+0)

Change 678040 **merged** by jenkins-bot:

[mediawiki/core@REL1_35] SECURITY: ContentModelChange: Check that user can create pages

https://gerrit.wikimedia.org/r/678040

Reedy changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2021-04-08 21:07:48 (UTC+0)

Xzonn added a comment. 2021-04-13 03:25:38 (UTC+0)

There is something wrong in the patch for 1.31. `$current` is not defined in line 174, it should be `$this->title`. And `getUserPermissionErrors` should be `getUserPermissionsErrors` in line 175.

gerritbot added a comment. 2021-04-13 03:40:57 (UTC+0)

Change 678686 had a related patch set uploaded (by Reedy; author: Reedy):

[mediawiki/core@REL1_31] Bug: T270988

https://gerrit.wikimedia.org/r/678686

ReleaseTaggerBot added a project: ~~**MW-1.31-release-notes**~~. 2021-04-13 05:00:27 (UTC+0)

sbassett moved this task from **In Progress** to **Our Part Is Done** on the **Security-Team** board. 2021-04-13 14:46:49 (UTC+0)

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

sbassett added a project: **Vuln-Misconfiguration**.