☑ CVE-2021-30159: Non-admin deleted enwiki page in fast double move

☑ Closed, Resolved 🌐 Public SECURITY

≡ Actions

Assigned To

tstarling

Authored By

PrimeHunter
2021-01-19 15:17:32 (UTC+0)

Tags

Security-Team (Our Part Is Done)
Security
MediaWiki-Page-rename (Backlog)
Platform Team Workboards (Clinic Duty Team) (Later)
MW-1.35-release (Blocker)
MW-1.31-release (Backlog)
Patch-For-Review
MW-1.37-notes (1.37.0-wmf.1; 2021-04-13)
MW-1.36-notes (Backlog)

Referenced Files

F34251709: 02-T272386-master.patch
2021-04-05 00:13:51 (UTC+0)

F34251708: 02-T272386-REL1_35.patch
2021-04-05 00:13:51 (UTC+0)

F34251710: 02-T272386-REL1_31.patch
2021-04-05 00:13:51 (UTC+0)

Subscribers

Aklapper
DannyS712
gerritbot
• holger.knust
PrimeHunter
Reedy
sbassett
tstarling

Description

Something odd happened when a non-admin moved https://en.wikipedia.org/wiki/Draft:Reign_of_X to https://en.wikipedia.org/wiki/Reign_of_X at 10:48 (UTC), 19 January 2021.
Two moves were registered within a second and all revisions of the moved page at the time were deleted. I have restored them. As far as I can tell from page histories, logs, and deleted page histories:

Draft:Reign_of_X had 38 edits at the time and had never been a redirect.
At 10:48 Mr Scribbles666, an autoconfirmed user with 11 edits, moved Draft:Reign_of_X to Reign_of_X which didn't exist at the time.
https://en.wikipedia.org/wiki/Special:Log/Mr_Scribbles666 says, in an admin account with time preference showing seconds and newest logs shown first:

2021-01-19T10:48:13 Mr Scribbles666 (talk|contribs|block) moved page Draft:Reign of X to Reign of X over redirect (thank)
2021-01-19T10:48:13 Mr Scribbles666 (talk|contribs|block) deleted redirect Reign of X by overwriting (G6: Deleted to make way for move) (view/restore) (thank)
2021-01-19T10:48:12 Mr Scribbles666 (talk|contribs|block) moved page Draft:Reign of X to Reign of X (revert) (thank)

"G6: Deleted to make way for move" is an automatic enwiki move summary made by https://en.wikipedia.org/wiki/MediaWiki:Delete_and_move_reason
These are the logs you would expect if the second move had been to a redirect to the source with no other edits in the page history, meaning non-admins can overwrite the redirect per
https://en.wikipedia.org/wiki/Wikipedia:Moving_a_page#Moving_over_a_redirect

At the time of the second move, Draft:Reign_of_X was a redirect left behind by the first move with no other page history. But MediaWiki claims Mr Scribbles666 deleted a redirect at the target Reign_of_X. At the time there should have been 38 revisions and never any redirect. As far as I can tell, MediaWiki deleted those 38 revisions with no other entry in the logs.

The first move, the alleged redirect deletion and the second move are consecutive within 31 total log entries that minute:
https://en.wikipedia.org/w/index.php?title=Special:Log&offset=202101191049&limit=31&type=&user=

The two moves are also recorded in the page history of the source where they have two consecutive oldid and are shown 1 second apart. There were 186 oldid that minute between these:
https://en.wikipedia.org/w/index.php?oldid=1001364985
https://en.wikipedia.org/w/index.php?oldid=1001365170

Mr Scribbles666 was understandibly confused. Reign_of_X was now a redirect to itself with no other page history. He moved it back to https://en.wikipedia.org/wiki/Draft:Reign_of_X. This was an allowed non-admin move over a redirect. He and 110.33.26.115 (probably himself) tried some edits there which didn't help. 110.33.26.115 then asked for help at
https://en.wikipedia.org/w/index.php?title=Wikipedia:Help_desk&oldid=1001379883#Please_get_back_the_original_version_of_Reign_of_X

That's where I came in. After a thorough investigation I restored all 39 deleted revisions at Reign_of_X. This was the 38 original revisions and 1 revision about the first move which was deleted in the second move.

I don't know whether Mr Scribbles666 did something unusual like double-clicking on "Move page". I didn't want to draw attention in case it could be abused so I didn't ask or indicate something strange was going on, and I'm filing this as a security bug.

Details

	Project	Subject
ᛘ	mediawiki/core	SECURITY: Non-admin deleted enwiki page in fast double move

mediawiki/core SECURITY: Non-admin deleted enwiki page in fast double move

mediawiki/core SECURITY: Non-admin deleted enwiki page in fast double move

mediawiki/core SECURITY: Non-admin deleted enwiki page in fast double move

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	tstarling	**~~T272386~~ CVE-2021-30159: Non-admin deleted enwiki page in fast double move**

PrimeHunter created this task. 2021-01-19 15:17:32 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-01-19 15:17:33 (UTC+0)

DannyS712 added a project: **MediaWiki-Page-rename**. 2021-01-19 21:49:47 (UTC+0)

DannyS712 added a subscriber: **DannyS712**.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2021-01-25 16:31:42 (UTC+0)

sbassett added a project: **Platform Engineering**.

sbassett added a subscriber: **sbassett**.

Platform Engineering - any interest in investigating this? Seems like a potential race condition?

• **holger.knust** triaged this task as *High* priority. 2021-01-26 21:22:48 (UTC+0)

• **holger.knust** edited projects, added **Platform Team Workboards (Clinic Duty Team)**; removed **Platform Engineering**.

• **holger.knust** added a subscriber: • **holger.knust**.

Is this an exploitable race condition?

• **holger.knust** moved this task from **Inbox** to **Later** on the **Platform Team Workboards (Clinic Duty Team)** board. 2021-01-26 21:23:08 (UTC+0)

tstarling added a subscriber: **tstarling**. Edited · 2021-01-26 22:58:00 (UTC+0)

MovePage::isValidMoveTarget() uses FOR UPDATE, but it's only called if Title::getArticleID() returns non-zero with no special flags. Then MovePage::moveToInternal() will delete the page if getArticleID(READ_LATEST) is non-zero. So it would seem that if the page is missing in the replica DB, isValidMove() will return true, and then moveToInternal() will unconditionally delete the page if it can be found in the master.

So it would seem that there's quite a wide exploitable window for unprivileged deletion of movable pages.

tstarling added a comment. 2021-01-29 04:48:53 (UTC+0)

I was able to reproduce this with a lagged slave by inserting a sleep at the start of ChronologyProtector::shutdown(). Using two separate client IPs probably also would have worked. With a single client IP, the second request needs to execute after the first move completes, but before the first request commits the ChronologyProtector position.

tstarling added a comment. 2021-01-29 05:50:50 (UTC+0)

This patch appears to be sufficient and should be deployed as a security update.

```
diff --git a/includes/MovePage.php b/includes/MovePage.php
index cdc994cab6..ffadf55586 100644
--- a/includes/MovePage.php
+++ b/includes/MovePage.php
@@ -231,7 +231,9 @@ class MovePage {

                if ( $this->oldTitle->equals( $this->newTitle ) ) {
                        $status->fatal( 'selfmove' );
-               } elseif ( $this->newTitle->getArticleID() && !$this->isValidMoveTarget() ) {
+               } elseif ( $this->newTitle->getArticleID( Title::READ_LATEST /* T272386 */ )
+                       && !$this->isValidMoveTarget()
+               ) {
                        // The move is allowed only if (1) the target doesn't exist, or (2) the target is a
                        // redirect to the source, and has no history (so we can undo bad moves right after
                        // they're done). If the target is a single revision redirect to a different page,
```

It seems fragile though, since READ_LATEST flags often get lost during refactoring, so I'm thinking about other redundant ways to ensure this bug doesn't recur.

sbassett added a subscriber: **Reedy**. 2021-01-29 20:25:17 (UTC+0)

> In ~~T272386#6786300~~, **@tstarling** wrote:
> *This patch appears to be sufficient and should be deployed as a security update.*

Thanks for the patch! **@Reedy** or I can plan to deploy this on Monday, February 1st during the next security window.

> *It seems fragile though, since READ_LATEST flags often get lost during refactoring, so I'm thinking about other redundant ways to ensure this bug doesn't recur.*

Sounds good. If these result in additional security patches, we can deploy those as well. Or if they're less sensitive and more code-hardening, I'd imagine they could just go through gerrit.

sbassett moved this task from **Watching** to **Security Patch To Deploy** on the **Security-Team** board. 2021-01-29 20:25:30 (UTC+0)

Reedy added projects: **MW-1.35-release**, **~~MW-1.31-release~~**. 2021-01-29 20:30:13 (UTC+0)

Reedy added a parent task: **~~T270459: Tracking bug for MediaWiki 1.31.13/1.35.2~~**. 2021-01-29 20:38:43 (UTC+0)

sbassett lowered the priority of this task from *High* to *Low*. 2021-02-01 22:13:45 (UTC+0)

sbassett moved this task from **Security Patch To Deploy** to **Our Part Is Done** on the **Security-Team** board.

Deployed the patch from ~~T272386#6786300~~ to wmf.27. Logs seem fine, though the actual fix might be difficult to test on a production wiki.

Reedy mentioned this in ~~T270459: Tracking bug for MediaWiki 1.31.13/1.35.2~~. 2021-03-30 00:40:04 (UTC+0)

Reedy assigned this task to **tstarling**. 2021-03-30 01:08:28 (UTC+0)

Reedy closed this task as *Resolved*. 2021-04-04 22:52:08 (UTC+0)

`git am -3` applies the master patch on REL1_35. Trivial rebase needed for REL1_31 (it's an `if` not an `elseif`, and code in a slightly different places)

Reedy added a comment. 2021-04-05 00:13:51 (UTC+0)

02-T272386-REL1_31.patch 959 B
Download

02-T272386-master.patch 924 B
Download

02-T272386-REL1_35.patch 1022 B
Download

Reedy renamed this task from *Non-admin deleted enwiki page in fast double move* to *CVE-2021-30159: Non-admin deleted enwiki page in fast double move*. 2021-04-06 19:14:08 (UTC+0)

Reedy added a subscriber: **gerritbot**. 2021-04-08 19:11:28 (UTC+0)

gerritbot added a comment. 2021-04-08 19:50:26 (UTC+0)

Change 678033 had a related patch set uploaded (by Reedy; author: Tim Starling):

[mediawiki/core@REL1_31] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678033

gerritbot added a project: **Patch-For-Review**. 2021-04-08 19:50:29 (UTC+0)

gerritbot added a comment. 2021-04-08 19:53:05 (UTC+0)

Change 678039 had a related patch set uploaded (by Reedy; author: Tim Starling):

[mediawiki/core@REL1_35] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678039

gerritbot added a comment. 2021-04-08 20:17:22 (UTC+0)

Change 678039 **merged** by jenkins-bot:

[mediawiki/core@REL1_35] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678039

gerritbot added a comment. 2021-04-08 20:21:07 (UTC+0)

Change 678033 **merged** by Reedy:

[mediawiki/core@REL1_31] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678033

gerritbot added a comment. 2021-04-08 20:43:11 (UTC+0)

Change 678074 had a related patch set uploaded (by Reedy; author: Tim Starling):

[mediawiki/core@master] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678074

Reedy changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2021-04-08 21:07:56 (UTC+0)

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

gerritbot added a comment. 2021-04-08 22:12:37 (UTC+0)

Change 678074 **merged** by jenkins-bot:

[mediawiki/core@master] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/678074

gerritbot added a comment. 2021-04-08 22:17:11 (UTC+0)

Change 677964 had a related patch set uploaded (by Reedy; author: Tim Starling):

[mediawiki/core@REL1_36] SECURITY: Non-admin deleted enwiki page in fast double move https://gerrit.wikimedia.org/r/677964

ReleaseTaggerBot added a project: ~~MW-1.37-notes (1.37.0-wmf.1; 2021-04-13)~~. 2021-04-08 23:00:37 (UTC+0)

gerritbot added a comment. 2021-04-09 00:39:48 (UTC+0)

Change 677964 **merged** by jenkins-bot:

[mediawiki/core@REL1_36] SECURITY: Non-admin deleted enwiki page in fast double move

https://gerrit.wikimedia.org/r/677964

ReleaseTaggerBot added a project: ~~MW-1.36-notes~~. 2021-04-09 01:00:37 (UTC+0)