A belated writeup of CVE-2022-28201 in MediaWiki

By Kunal Mehta

Sun 03 July 2022
in MediaWiki
tagged mediawiki, security, recursion, rust

In December 2021, I discovered CVE-2022-28201, which is that it's possible to get MediaWiki's `Title::newMainPage()` to go into infinite recursion. More specifically, if the local interwikis feature is configured (not used by default, but enabled on Wikimedia wikis), any on-wiki administrator could fully brick the wiki by editing the `[[MediaWiki:Mainpage]]` wiki page in a malicious manner. It would require someone with sysadmin access to recover, either by adjusting site configuration or manually editing the database.

In this post I'll explain the vulnerability in more detail, how Rust helped me discover it, and a better way to fix it long-term.

The vulnerability

At the heart of this vulnerability is `Title::newMainPage()`. The function, before my patch, is as follows (link):

Categories

- FLP
- Life
- MediaWiki
- Meta
- Music
- OSX
- Press
- Sports
- Tech

Social

Git
Mastodon
last.fm

```
public static function newMainPage( MessageLocalizer $localizer = null )
{
if ( $localizer ) {
$msg = $localizer->msg( 'mainpage' );
} else {
$msg = wfMessage( 'mainpage' );
}
$title = self::newFromText( $msg->inContentLanguage()->text() );
// Every page renders at least one link to the Main Page (e.g. sidebar).
// If the localised value is invalid, don't produce fatal errors that
// would make the wiki inaccessible (and hard to fix the invalid messag
e).
// Gracefully fallback...
if ( !$title ) {
$title = self::newFromText( 'Main Page' );
}
return $title;
}
```

It gets the contents of the "mainpage" message (editable on-wiki at MediaWiki:Mainpage), parses the contents as a page title and returns it. As the comment indicates, it is called on every page view and as a result has a built-in fallback if the configured main page value is invalid for whatever reason.

Now, let's look at how interwiki links work. Normal interwiki links are pretty simple, they take the form of `[[prefix:Title]]`, where the prefix is the interwiki name of a foreign site. In the default interwiki map, "wikipedia" points to `https://en.wikipedia.org/wiki/$1`. There's no requirement that the interwiki target even be a wiki, for example `[[google:search term]]` is a supported prefix and link.

And if you type in `[[wikipedia:]]`, you'll get a link to `https://en.wikipedia.org/wiki/`, which redirects to the Main Page. Nice!

Local interwiki links are a bonus feature on top of this to make sharing of content across multiple wikis easier. A local interwiki is one that maps to the wiki we're currently on. For example, you could type `[[wikipedia:Foo]]` on the English Wikipedia and it would be the same as just typing in `[[Foo]]`.

So now what if you're on English Wikipedia and type in `[[wikipedia:]]`? Naively that would be the same as typing `[[]]`, which is not a valid link.

So in c815f959d6b27 (first included in MediaWiki 1.24), it was implemented to have a link like `[[wikipedia:]]` (where the prefix is a local interwiki) resolve to the main page explicitly. This seems like entirely logical behavior and achieves the goals of local interwiki links - to make it work the same, regardless of which wiki it's on.

Except it now means that when trying to parse a title, the answer might end up being "whatever the main page is". And if we're trying to parse the "mainpage" message to discover where the main page is? Boom, infinite recursion.

All you have to do is edit "MediaWiki:Mainpage" on your wiki to be something like `localinterwiki:` and your wiki is mostly hosed, requiring someone to either de-configure that local interwiki or manually edit that message via the database to recover it.

The patch I implemented was pretty simple, just add a recursion guard with a hardcoded fallback:

```
public static function newMainPage( MessageLocalizer $localizer = null )
{
+ static $recursionGuard = false;
+ if ( $recursionGuard ) {
+ // Somehow parsing the message contents has fallen back to the
+ // main page (bare local interwiki), so use the hardcoded
+ // fallback (T297571).
+ return self::newFromText( 'Main Page' );
+ }
if ( $localizer ) {
$msg = $localizer->msg( 'mainpage' );
} else {
$msg = wfMessage( 'mainpage' );
}

+ $recursionGuard = true;
$title = self::newFromText( $msg->inContentLanguage()->text() );
+ $recursionGuard = false;

// Every page renders at least one link to the Main Page (e.g. sidebar).
// If the localised value is invalid, don't produce fatal errors that
```

Discovery

I was mostly exaggerating when I said Rust helped me discover this bug. I previously blogged about writing a MediaWiki title parser in Rust, and it was while working on that I read the title parsing code in MediaWiki enough times to discover this flaw.

A better fix

I do think that long-term, we have better options to fix this.

There's a new, somewhat experimental, configuration option called `$wgMainPageIsDomainRoot`. The idea is that rather than serve the main page from `/wiki/Main_Page`, it would just be served from `/`. Conveniently, this would mean that it doesn't actually matter what the name of the main page is, since we'd just have to link to the domain root.

There is an open request for comment to enable such functionality on Wikimedia sites. It would be a small performance win, give everyone cleaner URLs, and possibly break everything that expects `https://en.wikipedia.org/` to return a HTTP 301 redirect, like it has for the past 20+ years. Should be fun!

Timeline

- December 12, 2021: Reported in Phabricator as T297571. Included a patch as well.
- December 13, 2021: Fix deployed to Wikimedia sites
- March 31, 2022: Disclosed to the public, patches included in MediaWiki 1.35.6, 1.36.4 and 1.37.2 releases.

Acknowledgements

Thank you to Scott Bassett of the Wikimedia Security team for reviewing and deploying my patch, and Reedy for backporting and performing the security release.

Powered by pelican. Fork of pelican-sober theme. Content licensed as CC-BY-SA 4.0.