XSS on Pages viewed on Mobile (CVE-2020-26120)

☑ Closed, Resolved Public SECURITY

Actions

Assigned To

phuedx

Authored By

Reedy
2020-09-07 16:34:00 (UTC+0)

Tags

Security-Team (Incoming)
Security
Vuln-XSS
MobileFrontend (Backlog)
Mobile (MobileFrontend specific)
Readers-Web-Backlog (Kanbanana-FY-2020-21) (Doing)
MW-1.36-notes (1.36.0-wmf.9; 2020-09-15)

Referenced Files

F32249810: T262213.patch
2020-09-07 23:13:47 (UTC+0)

F32249763: T262213.patch
2020-09-07 22:06:55 (UTC+0)

F32249748: PageGateway.patch
2020-09-07 21:49:42 (UTC+0)

F32249749: 0001-Fix-XSS.patch
2020-09-07 21:49:42 (UTC+0)

Subscribers

Aklapper

CDanis

• dcipoletti

Jdlrobson

jeena

Niedzielski

nray

View All 12 Subscribers

Description

From Paser24 to security@

```
hi update:
I can create stored xss in my talk and discussion sections including title and text with xss payload and get stored xss.
let's reveal this valid report

Url vuln :
https://id.m.wikipedia.org/wiki/Pembicaraan_Pengguna:Longkali

Payload xss :
HACKED<br><br><center><font color="red">HACKED <br><br><img src=x onerror=alert(document.domain)><br><br><img src=x onerror=alert(document.domain)>
```

https://id.m.wikipedia.org/wiki/Pembicaraan_Pengguna:Longkali gives a lovely popup, https://id.wikipedia.org/wiki/Pembicaraan_Pengguna:Longkali doesn't

Introduced in 78f85803f64ae3ecedbecb38473ee70606fca5c9 as a fix for ~~T67042: Mobile Table of Contents double unescapes encoded characters~~ ... Fixing another XSS :) - rEMFR78f85803f64a: Fix XSS in section handling

Details

	Project	Subject
ᚹ	mediawiki/extensions/MobileFrontend	SECURITY: Remove regex section line replacement from PageGateway
ᚹ	mediawiki/extensions/MobileFrontend	SECURITY: Remove regex section line replacement from PageGateway
ᚹ	mediawiki/extensions/MobileFrontend	SECURITY: Remove regex section line replacement from PageGateway
ᚹ	mediawiki/extensions/MobileFrontend	SECURITY: Remove regex section line replacement from PageGateway

Customize query in gerrit

Related Objects

Search...

Task Graph Mentions

	Status	Assigned	Task
	✓ Resolved	Reedy	~~T256334~~ Release MediaWiki 1.31.9/1.34.3/1.35.0
●	✓ Resolved	sbassett	~~T256342~~ Write and send supplementary release announcement for extensions and skins with security patches (1.31.9/1.34.3/1.35.0)
	✓ Resolved	phuedx	~~T262213~~ XSS on Pages viewed on Mobile (CVE-2020-26120)

Reedy created this task. 2020-09-07 16:34:00 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2020-09-07 16:34:02 (UTC+0)

Reedy triaged this task as *High* priority. 2020-09-07 16:35:54 (UTC+0)

Reedy added projects: **Vuln-XSS**, **MobileFrontend**, **MinervaNeue**, **Mobile**.

Reedy added subscribers: **phuedx**, **Jdlrobson**, **Niedzielski** and **3 others**. 2020-09-07 17:01:18 (UTC+0)

Reedy updated the task description. **(Show Details)** 2020-09-07 17:08:33 (UTC+0)

ovasileva added a project: ~~**Readers-Web-Backlog (Kanbanana-FY-2020-21)**~~. 2020-09-07 17:08:41 (UTC+0)

ovasileva moved this task from **Needs Analysis** to **Ready for Development** on the ~~**Readers-Web-Backlog (Kanbanana-FY-2020-21)**~~ board.

Platonides added a subscriber: **Platonides**. 2020-09-07 17:37:27 (UTC+0)

I have simplified it to

```
== <center><img src=ignored onerror=alert(1)><img src=triggers onerror=alert(document.domain)> ==
```

You need a header with a center tag, and the onerror of the first img doesn't run, but the second does.

Only executed on mobile

Platonides added a comment. 2020-09-07 18:14:09 (UTC+0)

The first img doesn't really need any parameters:

```
==  <center><img><img src=zxcv onerror=throw(document.domain)> ==
```

This html is copied verbatim (but for the center) inside title of the href:

```
<a href="/w/index.php?title=Wikipedia:Sandbox/2020-09-07&amp;action=edit&amp;section=1" title="Edit section: <img><img src=zxcv onerror=throw(document.domain)>"
```

phuedx added a comment. 2020-09-07 18:14:50 (UTC+0)

Thanks @Platonides . Changing your example to

```
== <center><img src=ignored onerror=alert(1)><img src=triggers onerror=console.trace() ==
```

includes methods called `initialize`, `_postInitialize`, and `render`, which point to `View#render` in `MobileFrontend/src/mobile.startup/View.js` (https://gerrit.wikimedia.org/g/mediawiki/extensions/MobileFrontend/+/d4ae221a534a31d498aa3c8d86c796cf675c3e71/src/mobile.startup/View.js#252).

Platonides added a comment. 2020-09-07 18:20:32 (UTC+0)

If the page is protected (thus no edit section link), the XSS doesn't fire

Platonides renamed this task from *XSS on Mobile Talk Pages* to *XSS on Pages viewed on Mobile*. 2020-09-07 18:28:44 (UTC+0)

This also happens (in Mobile) when forcing a different skin, such as monobook or vector

Reedy removed a project: **MinervaNeue**. 2020-09-07 18:32:02 (UTC+0)

nray added a comment. Edited · 2020-09-07 18:47:50 (UTC+0)

It looks like this line 56 from `PageGateway.js` [1] is at least somewhat implicated in this:

```
section.line = section.line.replace( /<\/?a\b[^>]*>/g, '' );
```

Line 212 first gets the html from the `.mw-headline` selector [2] and then I think the `replace` call above is stripping tags and is making what was once inert HTML into an XSS attack vector

[1] https://github.com/wikimedia/mediawiki-extensions-MobileFrontend/blob/master/src/mobile.startup/PageGateway.js#L56
[2] https://github.com/wikimedia/mediawiki-extensions-MobileFrontend/blob/d4ae221a534a31d498aa3c8d86c796cf675c3e71/src/mobile.startup/PageGateway.js#L212

phuedx added a comment. 2020-09-07 18:53:07 (UTC+0)

To confirm what @nray says above:

```
<center>&lt;img src=ignored onerror=alert(1)&gt;&lt;img src=triggers onerror=console.trace();&gt;<span class="mw-editsection"><a href="/w/index.php?title=Talk:T262213&amp;action=edit&amp;section=1" title="Edit section: <img src=ignored onerror=alert(1)><img src=triggers onerror=console.trace();>" data-section="1" class="mw-ui-icon mw-ui-icon-element mw-ui-icon-wikimedia-edit-base20 edit-page mw-ui-icon-flush-right">Edit</a></span></center>
```

gets converted to

```
<center>&lt;img src=ignored onerror=alert(1)&gt;&lt;img src=triggers onerror=console.trace();&gt;<span class="mw-editsection"><img src=triggers onerror=console.trace();>" data-section="1" class="mw-ui-icon mw-ui-icon-element mw-ui-icon-wikimedia-edit-base20 edit-page mw-ui-icon-flush-right">Edit</span></center>
```

Platonides added a comment. 2020-09-07 19:36:57 (UTC+0)

probably fixed by changing to

```
section.line = section.line.replace(  /<\/?a\b("[^"]*"|[^>])*>/g, '' );
```

Or if we also want to take into account parameters using single quotes (which don't seem to be used)

```
section.line = section.line.replace(  /<\/?a\b("[^"]*"|'[^']*'|[^>])*>/g, '' );
```

CDanis added a subscriber: **CDanis**. 2020-09-07 21:26:23 (UTC+0)

phuedx added a comment. 2020-09-07 21:29:08 (UTC+0)

Brief update: There's a patch inbound from **@nray** . We've got a good handle on the issue.

Platonides added a comment. 2020-09-07 21:31:48 (UTC+0)

> In **~~T262213#6441220~~**, **@Platonides** wrote:
>
> ```
> section.line = section.line.replace(  /<\/?a\b("[^"]*"|'[^']*'|[^>])*>/g, '' );
> ```

After 2 hours fighting with mediawiki/MF/webpack: yes, it seems to work

Reedy added a comment. 2020-09-07 21:38:28 (UTC+0)

> In **~~T262213#6441309~~**, **@phuedx** wrote:
>
> *Brief update: There's a patch inbound from* ***@nray*** *. We've got a good handle on the issue.*

Thanks!

Do you need any help with deploying it etc? I'm on slack and irc. I am going to sort some food, but not far away from my keyboard.

Reedy added a parent task: **~~T256335: Tracking bug for MediaWiki 1.31.9/1.34.3/1.35.0~~**. 2020-09-07 21:49:33 (UTC+0)

Platonides added a comment. 2020-09-07 21:49:42 (UTC+0)

The basic fix I tried

PageGateway.patch 594 B
Download

plus the full change including the autogenerated files

0001-Fix-XSS.patch 1 KB
Download

nray added a comment. Edited · 2020-09-07 22:06:55 (UTC+0)

Thank you **@Platonides** for the patches! I think those patches fix the immediate issue, however after discussing this with **@phuedx** today, we'd both like to try removing the lines relating to the regex altogether as their continued usage is questionable at best. The small patch below applies this removal plus the required webpack build artifacts

T262213.patch 8 KB
Download

@Reedy could you help with the deploy? I do not have deploy rights

Platonides added a comment. 2020-09-07 22:12:18 (UTC+0)

Actually removing the regex seems preferable, indeed.
However, I think this may produce links inside links, which the previous code was trying to avoid?

Platonides added a comment. Edited · 2020-09-07 22:24:43 (UTC+0)

Testing it.

- It does fix the vulnerability
- If there is a header with links (e.g. `== [[page2]] [[page3]] [[page4]] ==`) you need to click it _outside_ the links to expand the section. Will that be confusing or people will manage fine? A question for usability team, I guess.

Seems to be the same that it did before, so I don't see what was that code supposed to be doing, then.

Reedy mentioned this in **~~T256335: Tracking bug for MediaWiki 1.31.9/1.34.3/1.35.0~~**. 2020-09-07 22:28:38 (UTC+0)

nray added a comment. 2020-09-07 22:33:53 (UTC+0)

@Platonides it's important to note that the code in question doesn't seem to affect the rendering of the section headings in the DOM regardless if the regex is there or not - that's server rendered. If you checkout master, the header with links still exists with your example. As far as I know, that's considered a feature (although it might be good to review that later on).

The closest thing we could find to a reason for the current code is found at commit sha **78f85803f64ae3ecedbecb38473ee70606fca5c9** which suggests it was originally intended to fix a previous XSS issue (ironically), but I'm not able to find a reason for its existence today.

Platonides added a comment. 2020-09-07 22:36:21 (UTC+0)

I thought it was removing links from headers, but it seems it was not doing anything ¯_(ツ)_/¯ (other than adding a security vulnerability).

Reedy added a comment. 2020-09-07 22:38:52 (UTC+0)

Good to go then?

@nray Yeah, I can deploy. Can you come on IRC for the deploy for some extra testing?

Platonides added a comment. 2020-09-07 22:39:26 (UTC+0)

My +2 to nray patch

nray added a comment. 2020-09-07 22:42:05 (UTC+0)

@Reedy yes, I'm on (`nray` is my nick)

Reedy edited parent tasks, added: ~~**T256342: Write and send supplementary release announcement for extensions and skins with security patches (1.31.9/1.34.3/1.35.0)**~~; removed: ~~**T256335: Tracking bug for MediaWiki 1.31.9/1.34.3/1.35.0**~~. 2020-09-07 22:57:36 (UTC+0)

Platonides added a comment. 2020-09-07 23:10:23 (UTC+0)

We should get a CVE for this extension vulnerability. This code has been here since 2014, and was added itself to avoid a XSS, so basically (assuming it wasn't safe before and something changed) **everyone** with MobileFrontend installed would be affected.

nray added a comment. Edited · 2020-09-07 23:13:47 (UTC+0)

Below adds patch on top of the origin/wmf/1.36.0-wmf.6 branch per **@Reedy** 's request

T262213.patch 8 KB
Download

Reedy added a comment. 2020-09-07 23:22:34 (UTC+0)

> In ~~**T262213#6441414**~~, **@Platonides** wrote:
>
> *We should get a CVE for this extension vulnerability. This code has been here since 2014, and was added itself to avoid a XSS, so basically (assuming it wasn't safe before and something changed)* ***everyone*** *with MobileFrontend installed would be affected.*

Yeah, that's why I tagged it against ~~**T256342: Write and send supplementary release announcement for extensions and skins with security patches (1.31.9/1.34.3/1.35.0)**~~. Between that and ~~**T256341: Obtain CVEs for 1.31.9/1.34.3/1.35.0 security releases**~~, Scott or I would usually do it as part of the process

Reedy assigned this task to **nray**. 2020-09-07 23:43:57 (UTC+0)

Reedy lowered the priority of this task from *High* to *Medium*.

Patch deployed.

Thanks to Sam and Nick for their help and the patch.

Knocking it down to normal for now

There's a patch for .7 in /srv/patches, as .7 is already branched, but not merged/deployed. .8 goes this week... .7 patch should work for .8 (I think it was made on master, and really, for .6 patch probably works... but we don't really care)

I'll followup on this tomorrow (or, rather, post sleep), and get it into master etc

Reedy added a parent task: ~~**T257976: 1.36.0-wmf.8 deployment blockers**~~. 2020-09-07 23:53:07 (UTC+0)

Just putting this as a subtask beneath ~~**T257976: 1.36.0-wmf.8 deployment blockers**~~ incase of security patch issues. Not actually blocker, but keeps the visibility incase of any issues

Releng: Feel free to just remove it if all is good :)

Reedy updated the task description. **(Show Details)** 2020-09-08 00:06:53 (UTC+0)

phuedx added a comment. Edited · 2020-09-08 14:36:33 (UTC+0)

Here's a brief writeup of the problem and why the fix makes sense:

1. The server was/is sending properly escaped content to the client
2. `mobile.init/mobile.init.js` calls `Skin::getSingleton`
3. `Skin::getSingleton` calls `currentPage::loadCurrentPage`
4. `loadCurrentPage` calls `PageGateway::getSectionsFromHTML`

`PageGateway::getSectionsFromHTML` finds all headings in the page content, extracts their HTML content (via `$( el ).html()`) and runs the following on each:

```
// Elsewhere
section.line = $( el ).html();

section.line = section.line.replace(  /<\/?a\b("[^"]*"|[^>])*>/g, '' )
```

5. The array returned by `PageGateway::getSectionsFromHTML` is used to construct an array of `Section` objects
6. The `Section` constructor function calls the `View` constructor function
7. The `View` constructor function:
   A. Calls `$.parseHTML( 'div' )` with the current document context (the default behaviour is to use a new document – see https://api.jquery.com/jQuery.parseHTML/ for detail)
   B. Renders an inline Mustache template that uses the value of `section.line` *unescaped*
   C. Sets the inner HTML of the element created in A to the rendered template

As far as **@nray** and I can tell, the `Section` objects and their underlying HTML elements are *never* used by `Skin::getSingleton`, `currentPage::loadCurrentPage`, or `PageGateway::getSectionsFromHTML`.

This vulnerability is a result of 4 and 7. In ~~**T262213#6441157**~~, I noted that

```
<center>&lt;img src=ignored onerror=alert(1)&gt;&lt;img src=triggers onerror=console.trace();&gt;<span class="mw-editsection"><a href="/w/index.php?title=Talk:T262213&amp;action=edit&amp;section=1" title="Edit
section: <img src=ignored onerror=alert(1)><img src=triggers onerror=console.trace();>" data-section="1" class="mw-ui-icon mw-ui-icon-element mw-ui-icon-wikimedia-edit-base20 edit-page mw-ui-icon-flush-
right">Edit</a></span></center>
```

(the HTML content of a heading) is converted to

```
<center>&lt;img src=ignored onerror=alert(1)&gt;&lt;img src=triggers onerror=console.trace();&gt;<span class="mw-editsection"><img src=triggers onerror=console.trace();>" data-section="1" class="mw-ui-icon mw-ui-
icon-element mw-ui-icon-wikimedia-edit-base20 edit-page mw-ui-icon-flush-right">Edit</span></center>
```

In 7C, the inner HTML of the newly created element in the current document is set to the above, the UA fails to fetch "/triggers", and the `error` event handler is run.

We could have fixed this by:

- Improving the regular expression in 4 (see ~~T262213#6441220~~)
- Override `View::parseHTML` in `Section` and don't pass `$.parseHTML` the current document as context
- Update `View::parseHTML` to the above for all `View` implementations
- Update `Section`'s template to escape the value of `section.line`

However, @nray and I ultimately decided to remove the regular expression in 4 because, as I've noted above, the `Section` objects and their underlying HTML elements are never used.

Here's a list of follow-up work that @nray and I identified:

- Update `SkinMinerva::doEditSectionLink` to render the `editsectionhint` message the same way that `Skin::doEditSectionLink` does
- Investigate and document whether it's necessary to model the sections of the page
  - If so, make the `Section` class a Plain Ol' JavaScript Object – a simple, side-effect-free model not a `View` implementation
- Investigate whether the current behaviour of `View::parseHTML` is the correct behaviour

phuedx added a comment. 2020-09-08 16:15:17 (UTC+0)

A couple more notes about the scope of the attack:

- It doesn't work when JavaScript is disabled
- It doesn't work when edit links aren't present (as @Platonides notes in ~~T262213#6441110~~)
- It works on all other mobile pageviews

Reedy added a comment. Edited · 2020-09-08 17:00:23 (UTC+0)

Thanks for the writeup.

As a plan for going forward...

Are you happy for the patch to go into gerrit? This is going to be needed "soon" as basically every patch that changes `resources/dist/mobile.common.js` and `resources/dist/mobile.common.js.map.json` is going to cause the security patch to not apply as part of the train. And as it's not just a trivial rebase (as it's a rebase + running webpack build stuff), it's more work than most patches.

As the extension isn't bundled in the tarball, and is already patched on WMF deployment, this is fairly usual practice. CVE and that disclosure can be done in the near future as part of the next security release where we generally announce these changes more widely (ala ~~T256342~~).

Then it's in master and can ride the train going forward.

I would appreciate some help doing the REL1_31/REL1_34/REL1_35 backports too if possible (again because you have dev/build environments setup for MF and webpack. I think REL1_31 is pre-webpack, so it looks like it should just need the change in `resources/mobile.startup/PageGateway.js`, not `mobile.common.js` / `mobile.common.js.map.json`). But with the task public and patches in gerrit, this can be done easily in the open. And then merged as appropriate when CI is happy.

What about this task to being opened up and made public? Any reason we cannot do that?

Where do you want to do the followup work identified? File seperate (security as approrpiate) tasks for them?

phuedx added a comment. 2020-09-08 17:11:50 (UTC+0)

> In ~~T262213#6443548~~, **@Reedy** wrote:
> *Are you happy for the patch to go into gerrit? This is going to be needed "soon" as basically every patch that changes `resources/dist/mobile.common.js` and `resources/dist/mobile.common.js.map.json` is going to cause the security patch to not apply as part of the train. And as it's not just a trivial rebase (as it's a rebase + running webpack build stuff), it's more work than most patches.*

I don't see any reason why the patch can't go into Gerrit and this task made public. ○ @dcipoletti ?

> *I would appreciate some help doing the REL1_31/REL1_34/REL1_35 backports too if possible (again because you have dev/build environments setup for MF and webpack. I think REL1_31 is pre-webpack, so it looks like it should just need the change in `resources/mobile.startup/PageGateway.js`, not `mobile.common.js` / `mobile.common.js.map.json`). But with the task public and patches in gerrit, this can be done easily in the open. And then merged as appropriate when CI is happy.*

I can help with this but it'll have to be tomorrow (BST).

> *Where do you want to do the followup work identified? File seperate (security as approrpiate) tasks for them?*

I can also file the tasks as they're all work for Readers Web. Again, this'll have to be tomorrow (BST).

Reedy added a comment. 2020-09-08 17:17:43 (UTC+0)

Yeah, no rush on my part. Definitely doesn't need doing "now".

We can certainly wait until tomorrow before putting patches into master in gerrit, opening up tasks etc :).

thcipriani added a subscriber: **thcipriani**. 2020-09-08 17:31:21 (UTC+0)

Branch was cut yesterday evening. The patch here (as was predicted) doesn't apply since it was generated by a build step that we don't have a good means of replicating. We can backport patches when they're available. For now continuing rollout to test wikis.

Reedy added a comment. 2020-09-08 17:46:07 (UTC+0)

https://github.com/wikimedia/mediawiki-extensions-MobileFrontend/blob/wmf/1.36.0-wmf.6/resources/dist/mobile.common.js - **3fb4e30** (25 Jul)
https://github.com/wikimedia/mediawiki-extensions-MobileFrontend/blob/wmf/1.36.0-wmf.7/resources/dist/mobile.common.js - **3fb4e30** (25 Jul)
https://github.com/wikimedia/mediawiki-extensions-MobileFrontend/blob/wmf/1.36.0-wmf.8/resources/dist/mobile.common.js - **da3edce** (3 Sep)

T262213.patch 8 KB
Download

should apply to .8, as I think it was done against master.

T262213.patch 8 KB
Download

definitely applies to .6, it should apply to .7 (which never really existed).

I put the first file into the .7 folder in /srv/patches, but didn't try to apply it as obviously .7 wasn't deployed.

Speaking to Jeena on IRC... It seems, for whatever reason, the patch from .6 was rolled forward into the .8 folder... Which is obviously wrong. But I don't know how the automated copying of security patches actually works... I'd presumed it would take it from .7 as the newest version... but seemingly not? If not.. Why does .7 exist on disk etc?

```
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.6/extensions/MobileFrontend/01-T262213.patch
13590667c0c0274009075cd92870a24e  1.36.0-wmf.6/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
847ad3264f5bd4a15d098e88c2f18920  1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
13590667c0c0274009075cd92870a24e  1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
```

Of course, things like this are evidence why these "build steps" are not helpful for security patches and wmf deployment

```
reedy@deploy1001:/srv/mediawiki-staging/php-1.36.0-wmf.8/extensions/MobileFrontend$ git am /srv/patches/1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
Applying: Remove regex section line replacement from PageGateway
reedy@deploy1001:/srv/mediawiki-staging/php-1.36.0-wmf.8/extensions/MobileFrontend$
```

Reedy added a comment. 2020-09-08 17:58:11 (UTC+0)

Tidied up the patches to match reality:

```
reedy@deploy1001:/srv/patches$ cp 1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
cp: cannot create regular file '1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch': Permission denied
reedy@deploy1001:/srv/patches$ ls -al 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
-rw-r--r-- 1 jhuneidi wikidev 8436 Sep  8 17:39 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ ls -al 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
-rw-rw-r-- 1 jhuneidi wikidev 8436 Sep  8 17:39 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ cp 1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ cp 1.36.0-wmf.6/extensions/MobileFrontend/01-T262213.patch 1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ git status
On branch master
Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        modified:   1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
        modified:   1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch

Untracked files:
  (use "git add <file>..." to include in what will be committed)

        1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch.failed

no changes added to commit (use "git add" and/or "git commit -a")
reedy@deploy1001:/srv/patches$ rm 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch.failed
rm: remove write-protected regular file '1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch.failed'? y
(failed reverse-i-search)`sha': nano T247149.^C
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
847ad3264f5bd4a15d098e88c2f18920  1.36.0-wmf.8/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
13590667c0c0274009075cd92870a24e  1.36.0-wmf.7/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ md5sum 1.36.0-wmf.6/extensions/MobileFrontend/01-T262213.patch
13590667c0c0274009075cd92870a24e  1.36.0-wmf.6/extensions/MobileFrontend/01-T262213.patch
reedy@deploy1001:/srv/patches$ git commit -a -m "Move T262213 .7 patch to .8, copy .6 patch to .7
>
> Bug: T262213"
[master 5335ca0] Move T262213 .7 patch to .8, copy .6 patch to .7
 2 files changed, 0 insertions(+), 0 deletions(-)
 rename {1.36.0-wmf.8 => 1.36.0-wmf.7}/extensions/MobileFrontend/01-T262213.patch (100%)
 rename {1.36.0-wmf.7 => 1.36.0-wmf.8}/extensions/MobileFrontend/01-T262213.patch (100%)
reedy@deploy1001:/srv/patches$
```

Jeena just said she accidentally copied the .6 patches to .8... which explains the problems/confusion with the patches.

Maybe something we should better document this, expecially in these cases where we still branch versions (ie .7 in this case), but don't stage/deplloy it to the deployment server and as such, WMF production.

No harm done :)

Reedy removed a parent task: ~~T257976: 1.36.0-wmf.8 deployment blockers~~. 2020-09-08 18:52:24 (UTC+0)

Untagging as blocking **~~T257976: 1.36.0-wmf.8 deployment blockers~~** as that is sorted now, and as such, doesn't block the train.

Aim is to get it into master this week, so shouldn't be a blocker for **~~T257977: 1.36.0-wmf.9 deployment blockers~~** either

nray moved this task from **Needs triage** to **MobileFrontend specific** on the **Mobile** board. 2020-09-08 19:02:57 (UTC+0)

phuedx added a comment. 2020-09-09 10:34:44 (UTC+0)

○ **@dcipoletti** has confirmed that, at least from our side, that this task can be opened up via Slack.

phuedx added a comment. 2020-09-09 10:35:44 (UTC+0)

AIUI backports to REL1_{31,34,35} still need to be done. Is that correct?

Reedy added a comment. 2020-09-09 12:27:36 (UTC+0)

> In **~~T262213#6446168~~**, **@phuedx** wrote:
> ○ ***@dcipoletti*** *has confirmed that, at least from our side, that this task can be opened up via Slack.*

Cool, we can do that as patches start going up

> In **~~T262213#6446169~~**, **@phuedx** wrote:
> *AIUI backports to REL1_{31,34,35} still need to be done. Is that correct?*

Yes please! Nicks original patch should apply cleanly to master. So should be fine to go straight into gerrit

T262213.patch 8 KB
Download

Typically, REL1_35 woudl've almost been ok with the .6 patch, but there's one commit more in 1.36 vs 1.35

Jdlrobson moved this task from **Ready for Development** to **Doing** on the ~~**Readers-Web-Backlog (Kanbanana-FY-2020-21)**~~ board. 2020-09-09 21:47:53 (UTC+0)

phuedx claimed this task. 2020-09-10 17:09:51 (UTC+0)

I'm doing the backports now...

jeena added a subscriber: **jeena**. Edited · 2020-09-10 23:12:13 (UTC+0)

Hi, just catching up on the comments here and clarifying that originally, the .6 version was copied into the .8 folder (talking this over later with thcipriani, we conjectured that this was because there was actually no .7 deploy)

Then, after talking to Reedy, when attempting to copy .7 version into the .8 folder, I mistakenly copied the .6 version again :(.

phuedx added a comment. 2020-09-11 11:42:08 (UTC+0)

> In ~~**T262213#6451366**~~, **@phuedx** wrote:
>
> *I'm doing the backports now...*

We're just waiting for confirmation that the original reporter wants to be credited (per https://www.mediawiki.org/wiki/Reporting_security_bugs#Crediting_Reporters).

Jdforrester-WMF added a project: ~~**MW-1.36-notes (1.36.0-wmf.9; 2020-09-15)**~~. 2020-09-11 16:09:58 (UTC+0)

phuedx added a comment. 2020-09-14 12:47:17 (UTC+0)

Patches to master, REL1_{31,34,35} have been submitted and merged.

Reedy closed this task as *Resolved*. 2020-09-14 15:13:41 (UTC+0)

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

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

sbassett mentioned this in ~~**T256342: Write and send supplementary release announcement for extensions and skins with security patches (1.31.9/1.34.3/1.35.0)**~~. 2020-09-14 15:54:48 (UTC+0)

sbassett mentioned this in ~~**T256341: Obtain CVEs for 1.31.9/1.34.3/1.35.0 security releases**~~. 2020-09-23 21:16:36 (UTC+0)

sbassett renamed this task from *XSS on Pages viewed on Mobile* to *XSS on Pages viewed on Mobile (CVE-2020-26120)*. 2020-09-28 16:54:49 (UTC+0)