☑ Unable to change visibility of log entries when MediaWiki:Mainpage uses Special:MyLanguage (CVE-2020-35477)

☑ Closed, Resolved   Public   SECURITY

≡ Actions

Assigned To

DannyS712

Authored By

Az1568
2018-10-01 18:21:04 (UTC+0)

Tags

- MediaWiki-Revision-deletion
- Regression
- Trust-and-Safety (Security/Abuse)
- WMF-General-or-Unknown
- MediaWiki-Logevents (Backlog)
- Security
- Security-Team (Watching)
- User-DannyS712 (Awaiting review and deployment)
- MW-1.36-notes (1.36.0-wmf.25; 2021-01-05)
- MW-1.31-release-notes
- MW-1.35-notes
- Vuln-Misconfiguration (Tracked)

Referenced Files

F32423162: T205908.patch
2020-11-02 12:59:29 (UTC+0)

F32419735: T205908.patch - old
2020-10-30 20:35:55 (UTC+0)

Subscribers

Aklapper

AIdnonymous

Amire80

Az1568

Base

BRPever

DannyS712

View All 26 Subscribers

Description

Steps to reproduce:
Set `MediaWiki:Mainpage` to `Special:MyLanguage/Main Page`
Go to a log entry on Special:Log and toggle the check box next to it
Click "Change visibility of selected log entries"

Expected result:
Revision deletion form is shown

Actual result:
User is redirect to main page with `action=historysubmit`

The same applies for trying to add/remove change tags

Original report:
Hi,

I've noticed today that when attempting to change the visibility of a log entry, I was no longer able to do so and redirected to Meta-Wiki's Main Page instead.

I started by selecting a log/checkbox here: https://meta.wikimedia.org/wiki/Special:Log/delete and then clicking change visibility.

It then redirects to https://meta.wikimedia.org/w/index.php?action=historysubmit&type=logging&revisiondelete=1&ids%5B28602506%5D=1
Which /should/ have loaded up the form to preform the change.

But instead the link just immediately redirects to https://meta.wikimedia.org/w/index.php?title=Main_Page&action=historysubmit

Details

	Project	Subject
⊁	mediawiki/core	SECURITY: Set a dummy title for Action buttons on Special:Log
⊁	mediawiki/core	SECURITY: Set a dummy title for Action buttons on Special:Log
⊁	mediawiki/core	SECURITY: Set a dummy title for Action buttons on Special:Log

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

Status	Assigned	Task
Resolved	Reedy	~~T263802~~ Release MediaWiki 1.31.11/1.35.1
Resolved	Reedy	~~T263803~~ Tracking bug for MediaWiki 1.31.11/1.35.1
Resolved	DannyS712	~~T205908~~ Unable to change visibility of log entries when MediaWiki:Mainpage uses Special:MyLanguage (CVE-2020-35477)

There are a very large number of changes, so older changes are hidden. Show Older Changes

Base added a comment. Edited · 2018-10-07 01:37:42 (UTC+0)

As a workaround it is still possible to use API for this. You can use your favourite bot framework or Special:APISandbox:

- https://meta.wikimedia.org/wiki/Special:ApiSandbox#action=query&format=xml&list=logevents&leuser=Base is used to get all the log actions with their ids (change Base to username of the user needed),
- https://meta.wikimedia.org/wiki/Special:ApiSandbox#action=revisiondelete&format=xml&type=logging&hide=comment%7Cuser copypaste here the `ids` retrieved above, make sure the `token` field is auto-filled.

stwalkerster added a subscriber: **stwalkerster**. 2018-10-07 23:01:05 (UTC+0)

TonyBallioni added a subscriber: **TonyBallioni**. 2018-10-08 00:05:37 (UTC+0)

Just as a note since there's been some confusion: this doesn't appear to be affecting en.wp

Base added a comment. 2018-10-09 23:24:24 (UTC+0)

It seems that to observe this bug the permissions needed for actual page usage are not necessary. You either get redirected to main page when this is observed, or get permission error.

With this I was able to see that besides wikimania2018 this is also observed on wikimania2017, wikimania2016, and wikimania2015, but not on other wikimania wikis.

Base added a project: **SRE**. 2018-10-09 23:28:01 (UTC+0)

This might as well be some faulty rewrite or other server misconfiguration, thus adding Operations.

Krenair removed a project: **SRE**. 2018-10-09 23:31:14 (UTC+0)

Krenair added a subscriber: **Krenair**.

This is likely between MW code and Wikimedia's MW config.

Krinkle added a subscriber: **Krinkle**. 2018-10-09 23:46:58 (UTC+0)

I can reproduce the observed issue at https://meta.wikimedia.org/w/index.php?action=historysubmit&type=logging&revisiondelete=1&ids%5B28602506%5D=1.

However, there is no redirect. It's a JavaScript address bar change. As such, not due to server or rewrite configuration. I looked at this because we're currently doing some maintenance on the Apache server configurations. And ruled it out as a possible cause.

Liuxinyu970226 moved this task from **To triage** to ~~**Special:Log**~~ on the **MediaWiki-Special-pages** board. 2018-10-10 12:32:14 (UTC+0)

jrbs added a project: **Trust-and-Safety**. 2018-10-25 00:56:46 (UTC+0)

jrbs added a subscriber: **jrbs**.

Matiia added a subscriber: **Matiia**. 2018-10-29 21:12:44 (UTC+0)

jrbs moved this task from **Backlog** to **Security/Abuse** on the **Trust-and-Safety** board. 2018-11-02 17:35:50 (UTC+0)

Base added a comment. 2018-11-03 19:21:23 (UTC+0)

With the above in mind I have decided to see what happens when I have JavaScript disabled. It looks that the URL indeed does not change. That being said I still see Main Page instead of the Special page.

Base added a project: **WMF-General-or-Unknown**. 2018-11-12 00:28:02 (UTC+0)

MarcoAurelio added a subscriber: **MarcoAurelio**. 2018-11-28 11:49:04 (UTC+0)

Mardetanha added a subscriber: **Mardetanha**. 2018-11-28 12:54:14 (UTC+0)

MF-Warburg added a subscriber: **MF-Warburg**. 2018-11-28 14:31:24 (UTC+0)

Teles added a subscriber: **Teles**. 2018-11-28 17:04:43 (UTC+0)

Jalexander set Security to Software security bug. 2018-11-28 19:45:51 (UTC+0)

Jalexander added a project: **acl*security**.

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

Jalexander added a subscriber: **Jalexander**.

moving to security given attack vector possibilites

Jalexander changed the visibility from "**Custom Policy**" to "**Custom Policy**". 2018-11-28 19:47:44 (UTC+0)

Trijnstel added a subscriber: **Trijnstel**. 2018-11-28 21:10:10 (UTC+0)

Anomie added a subscriber: **Anomie**. 2018-11-29 22:24:51 (UTC+0)

When visiting https://meta.wikimedia.org/w/index.php?action=historysubmit&type=logging&revisiondelete=1&ids%5B28602506%5D=1, `MediaWiki::parseTitle()` doesn't find any of various parameters that would specify the title, so it loads the main page as the title. Since September 27, 2018, at Meta that has been "Special:MyLanguage/Main Page".

Slightly later in the request, `Action::getActionName()` correctly determines that the action it wants is "revisiondelete", but then it hits a check that says if the current Title is a Special page it forces the 'view' action instead. Thus it acts like you actually visited https://meta.wikimedia.org/wiki/Special:MyLanguage/Main_Page and you wind up redirected to the main page.

I see that outreachwiki and wikimania2018wiki have MediaWiki:Mainpage set to similar values.

So the quick fix would be to not have MediaWiki:Mainpage be set to a Special page. Or if that's really wanted someone could figure out a code change to work around using Special:MyLanguage for the main page, e.g. resolving the RedirectSpecialPage in `Title::newMainPage()`, or set `$wgForceUIMsgAsContentMsg` on those wikis like Commons does.

Platonides added a subscriber: **Platonides**. 2018-11-29 23:29:15 (UTC+0)

I think that rather than loading the main page, and get confused when it's a special page, it should not attempt to use that as a title.

As an even faster workaround, I would try using https://meta.wikimedia.org/w/index.php?action=historysubmit&type=logging&revisiondelete=1&ids%5B28602506%5D=1&title=foo

Anomie added a comment. 2018-11-30 02:12:03 (UTC+0)

> In ~~T205908#4787688~~, **@Platonides** wrote:
> *I think that rather than loading the main page, and get confused when it's a special page, it should not attempt to use that as a title.*

The defaulting to the main page there is also what makes a link like `https://en.wikipedia.org/wiki/` go to the main page rather than being some sort of error. And in turn that's what makes an interwiki link to e.g. `[[en:]]` work to get to enwiki's main page without having to know that it's named "Main Page" rather than "Main page" or "Wikipedia:Main Page" or "Portal:Main page" or whatever.

Vogone closed this task as *Resolved*. 2018-11-30 11:45:21 (UTC+0)

Vogone claimed this task.

Thanks a lot for investigating the issue!

> In ~~T205908#4787443~~, **@Anomie** wrote:
> *So the quick fix would be to not have MediaWiki:Mainpage be set to a Special page. Or if that's really wanted someone could figure out a code change to work around using Special:MyLanguage for the main page, e.g. resolving the RedirectSpecialPage in* `Title::newMainPage()`*, or set* `$wgForceUIMsgAsContentMsg` *on those wikis like Commons does.*

That sounds like a terrible idea, since Commons's main page is broken. Just try setting your interface to a less common language (for example ht, but it is the case with all interface languages which do not have a main page translation available) and you will have a lot of fun with a red link main page.

Vogone reopened this task as *Open*. 2018-11-30 11:45:48 (UTC+0)

Vogone removed **Vogone** as the assignee of this task. 2018-11-30 11:51:14 (UTC+0)

MarcoAurelio added a comment. 2018-12-04 20:48:45 (UTC+0)

Hello. As an oversighter for Meta, I am unable to perform my duties due to this bug. Is there anything we can do locally, for now, to solve this? Thanks.

Anomie added a comment. 2018-12-04 20:51:49 (UTC+0)

As mentioned in ~~T205908#4787443~~, you could change https://meta.wikimedia.org/wiki/MediaWiki:Mainpage to not be referring to a Special page.

Krinkle edited projects, added **MediaWiki-Logevents**; removed **MediaWiki-Special-pages**. 2019-06-23 23:51:01 (UTC+0)

Base added a subscriber: **Kaganer**. 2019-10-14 20:18:41 (UTC+0)

Kaganer added a comment. 2019-10-29 13:00:19 (UTC+0)

There is any progress for resolving this bug?

Kaganer added a subscriber: **Amire80**. 2019-10-29 13:02:29 (UTC+0)

• **chasemp** added a project: **Security**. 2020-02-10 22:54:49 (UTC+0) ·

Krinkle removed a subscriber: **Krinkle**. 2020-02-10 23:26:04 (UTC+0)

Urbanecm merged a task: Restricted Task. 2020-02-20 09:23:01 (UTC+0)

Urbanecm added subscribers: **WhitePhosphorus**, **Urbanecm**, **DannyS712** and **2 others**.

• **chasemp** removed a project: **acl*security**. 2020-02-20 20:05:45 (UTC+0) ·

DannyS712 added a comment. 2020-07-04 14:46:50 (UTC+0)

No longer an issue on metawiki - see https://meta.wikimedia.org/w/index.php?title=Special:Log&dir=prev&offset=20200704131641&limit=2&type=delete
Can someone check outreach and wikimania2018wiki ?

Urbanecm closed this task as *Resolved*. 2020-07-04 19:21:11 (UTC+0)

Works for me, closing.

Urbanecm changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2020-07-04 19:21:35 (UTC+0)

Aklapper removed a subscriber: **Anomie**. 2020-10-16 17:40:36 (UTC+0) ·

Base added a comment. Edited · 2020-10-30 18:47:54 (UTC+0)

@Urbanecm, was it really resolved? It works on Meta since the main page target is temporarily (until this ticket is resolved[1]) pointing to Main Page, rather than Special:MyLanguage/Main Page

[1] https://meta.wikimedia.org/wiki/Special:Undelete/MediaWiki:Mainpage

DannyS712 added a comment. 2020-10-30 19:36:10 (UTC+0)

> In ~~T205908#6592350~~, **@Base** wrote:
> **@Urbanecm**, *was it really resolved? It works on Meta since the main page target is temporarily (until this ticket is resolved[1]) pointing to Main Page, rather than Special:MyLanguage/Main Page*

> *[1] https://meta.wikimedia.org/wiki/Special:Undelete/MediaWiki:Mainpage*

Can confirm that if `MediaWiki:Mainpage` is `Special:MyLanguage/Main Page` it still doesn't work (tested at https://meta.wikimedia.beta.wmflabs.org/wiki/MediaWiki:Mainpage)

DannyS712 reopened this task as *Open*. 2020-10-30 19:36:17 (UTC+0)

DannyS712 raised the priority of this task from *High* to *Needs Triage*.

DannyS712 triaged this task as *High* priority.

DannyS712 set Security to Software security bug.

DannyS712 added a project: **Security-Team**.

DannyS712 changed the visibility from "Public (No Login Required)" to "**Custom Policy**".

DannyS712 changed the subtype of this task from "Task" to "Security Issue".

->back to high, used the protect as security issue option to restrict visibility

DannyS712 renamed this task from *Unable to change visibility of log entries on at least metawiki, outreachwiki and wikimania2018wiki* to *Unable to change visibility of log entries when MediaWiki:Mainpage uses Special:MyLanguage*. 2020-10-30 19:39:05 (UTC+0)

DannyS712 updated the task description. **(Show Details)**

DannyS712 updated the task description. **(Show Details)** 2020-10-30 19:51:48 (UTC+0)

DannyS712 claimed this task. 2020-10-30 20:14:17 (UTC+0)

Restricted Application added a project: **User-DannyS712**. · View Herald Transcript 2020-10-30 20:14:19 (UTC+0)

DannyS712 added a project: **Patch-For-Review**. Edited · 2020-10-30 20:35:55 (UTC+0)

DannyS712 moved this task from **Unsorted** to **Awaiting review and deployment** on the **User-DannyS712** board.

T205908.patch - old 2 KB
Download

Discussed with **@Urbanecm** via IRC, scheduled for deployment Monday, November 02 19:00–20:00 UTC (Morning backport window)

DannyS712 added a comment. 2020-11-02 12:59:29 (UTC+0)

T205908.patch 2 KB
Download

Fixed commit message

Urbanecm added a comment. 2020-11-02 13:04:19 (UTC+0)

> In ~~**T205908#6595989**~~, **@DannyS712** wrote:
>
> ***T205908.patch*** *2 KB*
> *Download*
>
> *Fixed commit message*

Approved as of this patch.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2020-11-02 16:05:32 (UTC+0)

Urbanecm added a comment. 2020-11-02 19:08:24 (UTC+0)

Deployed and fixed for real

```
20:07 <Urbanecm> !log Deployed security fix for T205908
20:07 <+stashbot> Logged the message at https://wikitech.wikimedia.org/wiki/Server_Admin_Log
```

DannyS712 removed a project: **Patch-For-Review**. 2020-11-02 19:09:06 (UTC+0)

Urbanecm added a subscriber: **sbassett**. 2020-11-02 19:09:43 (UTC+0)

@sbassett Can you do the final honors please (CVE/backport)?

sbassett lowered the priority of this task from *High* to *Low*. Edited · 2020-11-02 20:43:47 (UTC+0)

sbassett added a parent task: ~~**T263803: Tracking bug for MediaWiki 1.31.11/1.35.1**~~.

> In ~~**T205908#6597765**~~, **@Urbanecm** wrote:
> ***@sbassett*** *Can you do the final honors please (CVE/backport)?*

As discussed over IRC, let's hold this task and patch for the next security release (~~**T263803**~~). Also setting task priority to **low** for now since the patch is in production.

Reedy mentioned this in ~~**T263803: Tracking bug for MediaWiki 1.31.11/1.35.1**~~. 2020-12-15 13:52:30 (UTC+0)

Reedy updated the task description. **(Show Details)**

Reedy closed this task as *Resolved*. 2020-12-15 13:56:21 (UTC+0)

Reedy added a subscriber: **Reedy**.

Patch applies cleanly to REL1_35 and REL1_31.

Closing for ease of tracking. Can/will be made public later

Reedy mentioned this in **~~T263809: Obtain CVEs for 1.31.11/1.35.1 security releases~~**. 2020-12-15 14:03:31 (UTC+0)

Reedy renamed this task from *Unable to change visibility of log entries when MediaWiki:Mainpage uses Special:MyLanguage* to *Unable to change visibility of log entries when MediaWiki:Mainpage uses Special:MyLanguage (CVE-2020-35477)*.
2020-12-16 19:56:37 (UTC+0)

Reedy changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2020-12-18 00:23:34 (UTC+0)

gerritbot added a comment. 2020-12-18 02:08:49 (UTC+0)

Change 650312 **merged** by jenkins-bot:
[mediawiki/core@master] SECURITY: Set a dummy title for Action buttons on Special:Log

https://gerrit.wikimedia.org/r/650312

ReleaseTaggerBot added a project: **~~MW-1.36-notes (1.36.0-wmf.25; 2021-01-05)~~**. 2020-12-18 03:00:32 (UTC+0)

Jdforrester-WMF added projects: **~~MW-1.31-release-notes~~**, **MW-1.35-notes**. 2020-12-21 19:33:14 (UTC+0)

sbassett added a project: **Vuln-Misconfiguration**. 2021-03-16 21:33:00 (UTC+0)

DannyS712 mentioned this in **T278376: Parser Use of RevisionRecord for a page that can't exist: (eg Special:MyLanguage/Main Page)**. 2021-03-24 19:29:20 (UTC+0)