

Bad english MediaWiki:Abusefilter-blocker breaks filters (CVE-2021-36126)

Closed, ResolvedPublicSECURITY

Actions

Assigned To

DannyS712

Authored By

DannyS712
2021-06-05 06:22:45 (UTC+0)

Tags

Security-Team

 (Our Part Is Done)

Security

User-DannyS712

 (Awaiting review and deployment)

AbuseFilter

 (Backlog)

Patch-For-Review

MW-1.37-notes

Referenced Files

F34483252: T284364-2.patch

2021-06-06 12:00:40 (UTC+0)

F34481301: T284364.patch

2021-06-05 06:28:48 (UTC+0)

Subscribers

Aklapper

Daimona

DannyS712

MarcoAurelio

sbassett

Description

If MediaWiki:Abusefilter-blocker is invalid in the content language, the filter user falls back to the English version, but that English version could also be invalid on a wiki - we should use Message::useDatabase() to ensure that the English version is fetched from the i18n files, rather than onwiki

Demo:

On beta metawiki, set <https://meta.wikimedia.beta.wmflabs.org/wiki/MediaWiki:Abusefilter-blocker> to Abuse Filter #test and trigger a filter that will try to block the user

Result:

```
[YLSNXJQ08eKxOGcOSgAEvwAAAA] /w/index.php?title=User:DannyS712/sandbox&action=submit TypeError: Argument 1 passed to MediaWiki\User\UserGroupManager::getUserGroups() must implement interface MediaWiki\User\UserIdentity, null given, called in /srv/mediawiki/php-master/extensions/AbuseFilter/includes/FilterUser.php on line 61
```

Backtrace:

```
from /srv/mediawiki/php-master/includes/user/UserGroupManager.php(651)
#0 /srv/mediawiki/php-master/extensions/AbuseFilter/includes/FilterUser.php(61): MediaWiki\User\UserGroupManager->getUserGroups(NULL)
#1 /srv/mediawiki/php-master/extensions/AbuseFilter/includes/Consequences/Consequence/BlockingConsequence.php(78): MediaWiki\Extension\AbuseFilter\FilterUser->getUser()
#2 /srv/mediawiki/php-master/extensions/AbuseFilter/includes/Consequences/Consequence/Block.php(62): MediaWiki\Extension\AbuseFilter\Consequences\Consequence\BlockingConsequence->doBlockInternal(string, integer, string, string, boolean, boolean)
#3 /srv/mediawiki/php-master/extensions/AbuseFilter/includes/Consequences/Consequence/Execute.php(317): MediaWiki\Extension\AbuseFilter\Consequences\Consequence\BlockingConsequence->execute()
```

Similar underlying cause as T53837

Details

Author Affiliation

Wikimedia Communities

Project	Subject
mediawiki/extensions/AbuseFilter	SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback
mediawiki/extensions/AbuseFilter	SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback

Customize query in Gerrit

Related Objects

Mentions

Mentioned In

T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)

Mentioned Here

T27623: automatic unicode conversion for Malayalam makes it difficult to link to external sites using old unicode sequences; want a tag to supress conversion

T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)

T160666: AbuseFilter should use the same account name on all WMF projects

DannyS712 created this task.

2021-06-05 06:22:45 (UTC+0)

Restricted Application added a project: User-DannyS712.

· View Herald Transcript

2021-06-05 06:22:46 (UTC+0)

Restricted Application added a subscriber: Aklapper.


· View Herald Transcript

DannyS712 added a project: AbuseFilter.

2021-06-05 06:23:04 (UTC+0)

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

2021-06-05 06:28:48 (UTC+0)

 **DannyS712** added a subscriber: **Daimona.**

^ simple patch to just add a `->useDatabase(false)` call, @Daimona would you mind reviewing?

 Daimona added a comment. 2021-06-05 13:37:19 (UTC+0)

In ~~T284364#7135981~~, @DannyS712 wrote:

^ simple patch to just add a `->useDatabase(false)` call, @Daimona would you mind reviewing?

-1, line is too long and will fail PHPCS once on gerrit. Aside from that, I think the fix is OK for the short term (long term solution is to make the name non-customizable)

T160666 might be of interest.

● **DannyS712** added a comment. Edited · 2021-06-06 12:00:40 (UTC+0)

@Daimona I've fixed the too long line

● **Daimona** added a comment. 2021-06-06 16:37:39 (UTC+0)

Approved.

 DannyS712 added a comment. 2021-06-06 16:51:03 (UTC+0)


In ~~T284364#7136885~~, @Daimona wrote:

Approved.

Thanks - there is a security window on Monday, should we plan on deploying it then? I can add a link to this task to the wikitech deployments page

→ sbassett triaged this task as *High* priority. 2021-06-07 15:52:17 (UTC+0)

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board.

 sbassett added a subscriber: sbassett. 2021-06-07 16:44:22 (UTC+0)

In ~~T284364#7136905~~, @DannyS712 wrote:

In ~~T284364~~#7136885, @Daimona wrote:

Approved.

Thanks - there is a security window on Monday, should we plan on deploying it then? I can add a link to this task to the wikitech deployments page

+1 to the patch, I can deploy it today during the security window. Would be great if someone could be around to help test the ext, otherwise I'll just keep an eye on logstash.

 sbassett claimed this task. 2021-06-07 16:44:32 (UTC+0)

sbassett mentioned this in ~~F279733~~. Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1). 2021-06-07 21:14:53 (UTC+0)

 DannyS712 removed a project: **Patch-For-Review**. 2021-06-07 21:16:33 (UTC+0)

(since stashbot isn't here)

📄 Mentioned in SAL (#wikimedia-operations) [2021-06-07T21:12:32Z] <sbassett> Deployed security patch for **T284364**

 sbassett added a comment. Edited - 2021-06-07 21:17:10 (UTC+0)

Deployed during the 2021-06-07 security window. Tested by @DannyS712. Tracking at T276237 and T279733

 sbassett moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board. 2021-06-29 15:28:29 (UTC+0)

👇 **sbassett** lowered the priority of this task from *High* to *Low*. 2021-07-01 22:35:48 (UTC+0)

 **sbassett** changed Author Affiliation from N/A to Wikimedia Communities.

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

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

 gerritbot added a comment. 2021-07-01 22:36:06 (UTC+0)


Change 702765 had a related patch set uploaded (by SBassett; author: DannyS712):

[mediawiki/extensions/AbuseFilter@master] SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback

<https://gerrit.wikimedia.org/r/702765>


 **gerritbot** added a project: **Patch-For-Review**. 2021-07-01 22:36:07 (UTC+0)

Change 702721 had a related patch set uploaded (by SBassett; author: DannyS712):
[mediawiki/extensions/AbuseFilter@REL1_36] SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback
<https://gerrit.wikimedia.org/r/702721>


 **gerritbot** added a comment. 2021-07-02 15:46:54 (UTC+0)


Change 702765 **merged** by jenkins-bot:
[mediawiki/extensions/AbuseFilter@master] SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback
<https://gerrit.wikimedia.org/r/702765>


 **ReleaseTaggerBot** added a project: ~~MW 1.37 notes (1.37.0 wmf 14, 2021-07-12)~~. 2021-07-02 16:00:18 (UTC+0)


 **gerritbot** added a comment. 2021-07-02 16:10:59 (UTC+0)

Change 702721 **merged** by jenkins-bot:
[mediawiki/extensions/AbuseFilter@REL1_36] SECURITY: Avoid database for MediaWiki:Abusefilter-blocker fallback
<https://gerrit.wikimedia.org/r/702721>

 **sbassett** renamed this task from *Bad english MediaWiki:Abusefilter-blocker breaks filters* to *Bad english MediaWiki:Abusefilter-blocker breaks filters (CVE-2021-36126)*. 2021-07-02 20:03:42 (UTC+0)

 **sbassett** closed this task as *Resolved*. 2021-07-02 20:14:51 (UTC+0)

 **sbassett** reassigned this task from **sbassett** to **DannyS712**.

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