

CVE-2021-30158: Allow blocked users to access Special:ResetTokens

Closed, Resolved

Public

SECURITY

Actions

Assigned To

matmarex

Authored By

IN

2021-03-10 07:56:57 (UTC+0)

Tags

Security-Team

 (Our Part Is Done)

MediaWiki-Watchlist

 (Backlog)

Growth-Team

 (Inbox)

MW-1.36-notes

 (1.36.0-wmf.35; 2021-03-16)

MW-1.31-release-notes

MW-1.35-notes

Privacy

Security

SecTeam-Processed

 (Completed)

Vuln-DoS

 (Tracked)

Referenced Files

F34149902: 0001-Allow-blocked-users-to-access-Special-ResetTokens.patch

2021-03-10 16:19:36 (UTC+0)

Subscribers

Aklapper

DannyS712

gerritbot

IN

Legoktm




matmarex

sbassett

Description

If users knowing his watchlist feed then being able to view his watchlist an unlimited number of times before block end his, And the user that is blocked must accept only, because he does not have method to be able to reset key.

Details

Project	Subject
 mediawiki/core	Allow blocked users to access Special:ResetTokens
 mediawiki/core	Allow blocked users to access Special:ResetTokens
 mediawiki/core	Allow blocked users to access Special:ResetTokens




Customize query in gerrit


Related Objects



Q Search...


Task Graph


Mentions



Status	Assigned	Task
 Resolved	Reedy	<del>T270458</del> Release MediaWiki 1.31.13/1.35.2
 Resolved	Reedy	<del>T270459</del> Tracking bug for MediaWiki 1.31.13/1.35.2
 Resolved	matmarex	<del>T277009</del> CVE-2021-30158: Allow blocked users to access Special:ResetTokens


 IN created this task. 2021-03-10 07:56:57 (UTC+0)


  Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-03-10 07:56:59 (UTC+0)

 IN renamed this task from *If a user shares his watchlist key before being blocked, his watchlist key cannot be modified in any way during the duration of the block.* to *If a user shares his watchlist key before being blocked, his watchlist key cannot be modified in any way during the duration of the block.* 2021-03-10 07:57:46 (UTC+0)

 IN added a project: **MediaWiki-Watchlist**.

  Restricted Application added a project: **Growth-Team**. · View Herald Transcript 2021-03-10 07:57:47 (UTC+0)

 **Aklapper** changed the task status from *Open* to *Stalled*. 2021-03-10 08:11:15 (UTC+0)

Hi  **@IN** , thanks for taking the time to report this. Please always follow [https://www.mediawiki.org/wiki/How\\_to\\_report\\_a\\_bug](https://www.mediawiki.org/wiki/How_to_report_a_bug) and provide:

- a clear and complete list of exact steps to reproduce the situation, step by step, so that nobody needs to guess or interpret how you performed each step,
- what happens after performing these steps to reproduce,
- what you expected to happen instead and why you think that is a Security problem,
- a full link to a web address where the issue can be seen.

In separate sections.

You can edit the task description by clicking [✎ Edit Task](#) . Ideally, a good description should allow any other person to follow these steps (without having to interpret steps) and see the same results. Problems that others can reproduce can get fixed faster. Thanks again.

✎ **Aklapper** renamed this task from *If a user shares his watchlist key before being blocked, his watchlist key cannot be modified in any way during the duration of the block* to *If a user shares their watchlist token before being blocked, their token cannot be modified during the duration of the block*. 2021-03-10 08:11:43 (UTC+0)

💬 **IN** added a comment. Edited · 2021-03-10 08:22:44 (UTC+0)

The specific steps are as follows:

0. Share your own feed token on test wiki.

1. Block yourself on testwiki.
2. Visit <https://w.wiki/35Bb> .
3. You can see:

*Your username or IP address has been blocked.*

*The block was made by `yourself` . The reason given is test for **T277009***

*Start of block: just now*

*Expiration of block: [...]*

*Intended blockee: `yourself`*

*You can contact `yourself` or another administrator to discuss the block. You can use the "Email this user" feature if a valid email address is specified in your preferences and you have not been blocked from using it. Your current IP address is [...], and the block ID is #[...]. Please include all above details in any queries you make.*

And you can't reset your key because it's overwritten by block notice, It cannot be modified under any circumstances.

💬 **Aklapper** added a comment. 2021-03-10 08:25:56 (UTC+0)

*And you can't reset your key because it's overwritten by block notice.*

Why would you want to reset your token if you are blocked anyway?

How is that a security issue, see [https://www.mediawiki.org/wiki/Reporting\\_security\\_bugs#What\\_is\\_Considered\\_A\\_Security\\_Issue](https://www.mediawiki.org/wiki/Reporting_security_bugs#What_is_Considered_A_Security_Issue) ?

Please read my previous comment, which asked for "what you expected to happen instead and why you think that is a Security problem".

💬 **IN** added a comment. 2021-03-10 08:30:18 (UTC+0)

In **T277009#6899506**, @Aklapper wrote:

*And you can't reset your key because it's overwritten by block notice.*

*Why would you want to reset your token if you are blocked anyway?*

*How is that a security issue, see [https://www.mediawiki.org/wiki/Reporting\\_security\\_bugs#What\\_is\\_Considered\\_A\\_Security\\_Issue](https://www.mediawiki.org/wiki/Reporting_security_bugs#What_is_Considered_A_Security_Issue) ?*

*Please read my previous comment, which asked for "what you expected to happen instead and why you think that is a Security problem".*

Because the token has already been shared. This is a security issue because the user's token is already publicly visible but he doesn't have the ability to reset the token, because he happens to be blocked. In other words, if the token of a blocked user is made public, the blocked user cannot change the token in any case.

💬 **Aklapper** added a comment. 2021-03-10 10:09:03 (UTC+0)

In **T277009#6899512**, @IN wrote:

*Because the token has already been shared. This is a security issue because the user's token is already publicly visible*

@IN : Where exactly is the token publicly visible to someone who is not the user themselves? Where can I see your token, basically? Please follow [https://www.mediawiki.org/wiki/How\\_to\\_report\\_a\\_bug](https://www.mediawiki.org/wiki/How_to_report_a_bug) and provide complete steps to reproduce some situation. Thanks.

💬 **Aklapper** added a comment. 2021-03-10 10:11:57 (UTC+0)

@IN : You linked to <https://test.wikipedia.org/w/index.php?title=Special:ResetTokens&returnto=Special%3APreferences&uselang=en> (please avoid obfuscating links).

That page says "You can reset tokens which allow access to certain private data associated with your account here. You should do it if you accidentally shared them with someone or if your account has been compromised." I do not see a **Security** issue here, but a **Privacy** issue. If you see a Security issue, then please see [https://www.mediawiki.org/wiki/Reporting\\_security\\_bugs#What\\_is\\_Considered\\_A\\_Security\\_Issue](https://www.mediawiki.org/wiki/Reporting_security_bugs#What_is_Considered_A_Security_Issue) and explain what the Security issue is. Thanks.

👤 **Legoktm** added a subscriber: **Legoktm**. 2021-03-10 16:16:07 (UTC+0)

We should definitely allow blocked users to use Special:ResetTokens. I'm not sure exactly if I'd consider it a **Vuln-Infoleak** since it relies on the watchlist token being distributed/compromised but it's something we should allow for. I think this was accidental rather than intentional, it just uses the default from FormSpecialPage.

In **T277009#6899764**, @Aklapper wrote:

In **T277009#6899512**, @IN wrote:

*Because the token has already been shared. This is a security issue because the user's token is already publicly visible*

@IN : Where exactly is the token publicly visible to someone who is not the user themselves? Where can I see your token, basically? Please follow [https://www.mediawiki.org/wiki/How\\_to\\_report\\_a\\_bug](https://www.mediawiki.org/wiki/How_to_report_a_bug) and provide complete steps to reproduce some situation. Thanks.

Watchlist tokens allow access to your watchlist, so you can use them for RSS feeds, or even have a shared watchlist amongst multiple users. The token should be unguessable, but the more likely scenario here is that you share it with someone or accidentally leak it and need to reset it. Special:ResetTokens is the way to do that, except it currently disallows blocked users from using it.

👤 **matmarex** added a subscriber: **matmarex**. 2021-03-10 16:19:36 (UTC+0)

Patch:

0001-Allow-blocked-users-to-access-Special-ResetTokens.patch

930 B

Download

(I can submit to Gerrit instead if this isn't considered a security issue)

Legoktm added a comment.

2021-03-10 16:33:41 (UTC+0)

In ~~T277009#6901149~~, @matmarex wrote:

Patch:

0001-Allow-blocked-users-to-access-Special-ResetTokens.patch

930 B

Download

Code-Review +2

DannyS712 added a subscriber: DannyS712.

2021-03-10 16:34:01 (UTC+0)

In ~~T277009#6901149~~, @matmarex wrote:

Patch:

0001-Allow-blocked-users-to-access-Special-ResetTokens.patch

930 B

Download

(I can submit to Gerrit instead if this isn't considered a security issue)

Untested, but makes sense - assuming that Jenkins wouldn't object, +2 from me - not sure if this needs to be deployed as a security patch or can go through gerrit, I think gerrit would be fine (please add me as a reviewer if done on gerrit)

sbassett triaged this task as *Medium* priority.

2021-03-10 16:58:24 (UTC+0)

sbassett moved this task from *Incoming* to *Watching* on the *Security-Team* board.

sbassett added a subscriber: sbassett.

In ~~T277009#6901240~~, @DannyS712 wrote:

Untested, but makes sense - assuming that Jenkins wouldn't object, +2 from me - not sure if this needs to be deployed as a security patch or can go through gerrit, I think gerrit would be fine (please add me as a reviewer if done on gerrit)

IMO, this is **low-risk** to push through gerrit, so feel free to do that.

matmarex added a project: Patch-For-Review.

2021-03-10 17:53:00 (UTC+0)

<https://gerrit.wikimedia.org/r/c/mediawiki/core/+670546>

Jdforrester-WMF added a project: ~~MW-1.36-notes (1.36.0-wmf.35, 2021-03-10)~~.

2021-03-10 19:24:21 (UTC+0)

DannyS712 assigned this task to matmarex.

2021-03-10 19:48:29 (UTC+0)

DannyS712 removed a project: Patch-For-Review.

Patch was merged

sbassett added a comment.

2021-03-10 20:12:52 (UTC+0)

I feel like this doesn't need a pick/deploy to wmf.34 and can wait until next week, unless anyone has more serious concerns.

sbassett mentioned this in ~~T270459-Tracking bag for MediaWiki 1.34.13/1.35.2~~.

2021-03-10 20:15:05 (UTC+0)

Jdforrester-WMF added projects: ~~MW-1.34-release-notes~~, ~~MW-1.35-notes~~.

2021-03-10 23:17:09 (UTC+0)

IN renamed this task from *If a user shares their watchlist token before being blocked, their token cannot be modified during the duration of the block to Allow blocked users to access Special:ResetTokens*.

Edited - 2021-03-11 07:47:00 (UTC+0)

IN updated the task description. (Show Details)

I think this task should be a feature request, not a security issue. Can someone change it to FEATURE?

Because it's really a privacy issue, so please do not expose this task until a new version is released. After the new version is released, the task is over, so it can be make public.

IN edited projects, added *Privacy*; removed *Security*.

2021-03-11 07:55:09 (UTC+0)

sbassett added projects: *Security*, *SecTeam-Processed*.

2021-03-11 16:50:11 (UTC+0)

In ~~T277009#6903536~~, @IN wrote:

I think this task should be a feature request, not a security issue. Can someone change it to FEATURE?

It's a lightweight user Vuln-DoS so we can keep the Security label.

Because it's really a privacy issue, so please do not expose this task until a new version is released. After the new version is released, the task is over, so it can be make public.

Yes, we can keep this task protected probably until Thursday of next week, after c954cc85ea is cut with *wmf.35* and makes it to all wiki groups. The gerrit change set is already public, of course, but this is low-risk enough imo, and the change set discreet enough, that it shouldn't be problematic.

sbassett added a project: *Vuln-DoS*.

2021-03-17 15:09:10 (UTC+0)

IN added a comment.

2021-03-19 12:37:47 (UTC+0)

Is this mission over now?

 **Aklapper** added a comment. 2021-03-19 12:40:25 (UTC+0)

 **@IN**: ? What "mission"?

Was that a question whether to resolve this ticket now that <https://gerrit.wikimedia.org/r/c/mediawiki/core/+670546> has been merged?


 **sbassett** closed this task as *Resolved*. 2021-03-19 15:48:33 (UTC+0)

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

In ~~T277009#6928372~~, **@IN** wrote:


*Is this mission over now?*

If you mean "can we resolve the task and make it public because the patch is now on `wmf-3.5` and deployed to all wikis?", the answer to that question is yes. I'll go ahead and do that now.

 **sbassett** changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2021-03-19 15:48:51 (UTC+0)

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

 **Reedy** added a parent task: ~~T270459 - Tracking bug for MediaWiki 1.34.13/1.35.2~~. 2021-03-30 00:42:53 (UTC+0)

 **Reedy** renamed this task from *Allow blocked users to access Special:ResetTokens* to *CVE-2021-30158: Allow blocked users to access Special:ResetTokens*. 2021-04-06 19:13:40 (UTC+0)

 **Reedy** added a subscriber: **gerritbot**. 2021-04-08 19:11:22 (UTC+0)