Special:GlobalUserRights reveals existence of globally suppressed users (CVE-2021-36127)

Closed, Resolved   Public   SECURITY

Actions

Assigned To

Zabe

Authored By

Zabe
2021-06-20 16:59:21 (UTC+0)

Tags

Security-Team (Our Part Is Done)

Security

Vuln-Infoleak

MediaWiki-extensions-CentralAuth (Incoming)

MW-1.37-notes (1.37.0-wmf.14; 2021-07-12)

Referenced Files

F34532053: 0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch
2021-06-29 21:32:24 (UTC+0)

F34524186: 0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch
2021-06-23 22:34:59 (UTC+0)

F34520123: 0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch
2021-06-22 10:19:54 (UTC+0)

F34515858: 0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch
2021-06-20 17:01:35 (UTC+0)

F34515795: nonexisting.png
2021-06-20 16:59:21 (UTC+0)

F34515796: suppressed.png
2021-06-20 16:59:21 (UTC+0)

Subscribers

Aklapper

CptViraj

DannyS712

Mstyles

sbassett

ST47

Zabe

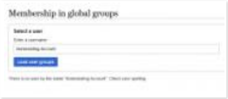
Description

Globally suppressed users should be treated like they don't exist, but Special:GlobalUserRights reveals the existence of them. See related ~~T276306: CVE-2021-30156: Special:Contributions toolbar reveals existence of hidden users~~ and ~~T270453: CVE-2021-30153: ApiVisualEditor leaks info about hidden users~~.

Steps to reproduce

1. Globally suppress an account, e.g. `Some Account`.
2. Goto `Special:GlobalUserRights/Some Account`, where `Some Account` is that globally suppressed account.

Expected result

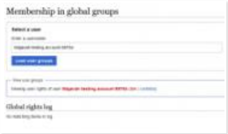


Membership in global groups

Select a user

Load user groups

Actual result



Membership in global groups

Select a user

Load user groups

Global rights log

(screenshots were taken on beta cluster)

Details

Author Affiliation
Wikimedia Communities

	Project	Subject
ᚹ	mediawiki/extensions/CentralAuth	SECURITY: Act like users don't exist if hidden from viewer
ᚹ	mediawiki/extensions/CentralAuth	SECURITY: Act like users don't exist if hidden from viewer
ᚹ	mediawiki/extensions/CentralAuth	SECURITY: Act like users don't exist if hidden from viewer
ᚹ	mediawiki/extensions/CentralAuth	SECURITY: Act like users don't exist if hidden from viewer

Customize query in gerrit

Related Objects

Mentions Duplicates

Mentioned In

~~T298784: Security Issue Access Request for Zabe~~
~~T260863: Globally hidden usernames can be enumerated by unauthenticated users by crawling Special:GlobalUserRights with user IDs~~
~~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

~~T260863: Globally hidden usernames can be enumerated by unauthenticated users by crawling Special:GlobalUserRights with user IDs~~
~~T192957: "Account is hidden from public lists" is misleading~~
~~T270453: CVE-2021-30153: ApiVisualEditor leaks info about hidden users~~
~~T276306: CVE-2021-30156: Special:Contributions toolbar reveals existence of hidden users~~

Zabe created this task. 2021-06-20 16:59:21 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-06-20 16:59:22 (UTC+0)

Zabe added a comment. Edited · 2021-06-20 17:01:35 (UTC+0)

This patch should do the job:

0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch 1 KB
Download

(untested, as I do not have a local CentralAuth setup)

Zabe added projects: ~~**User-Zabe**~~, **Vuln-Infoleak**, **MediaWiki-extensions-CentralAuth**. 2021-06-20 17:02:18 (UTC+0)

Zabe added a project: **Patch-For-Review**. 2021-06-20 17:05:35 (UTC+0)

DannyS712 added a subscriber: **DannyS712**. 2021-06-20 19:26:03 (UTC+0)

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board. 2021-06-21 15:53:29 (UTC+0)

Mstyles added a subscriber: **Mstyles**. Edited · 2021-06-21 21:01:09 (UTC+0)

@Zabe this patch works for globally suppressed users, but there are some users who have both `gu_status` and `lists` as attributes, in the database still have the same error message. Not sure if the patch should cover those users as well. Another patch can be submitted if that's the case. More context for hidden lists -> ⚓ https://phabricator.wikimedia.org/T192957

Mstyles moved this task from **Security Patch To Deploy** to **Our Part Is Done** on the **Security-Team** board. 2021-06-21 21:15:50 (UTC+0)

Security patch deployed June 21, 2021 -> https://sal.toolforge.org/log/Q1RpMHoBa_6PSCT9zC0q

sbassett removed a project: **Patch-For-Review**. 2021-06-21 21:16:52 (UTC+0)

Mstyles mentioned this in ~~**T279733: Write and send supplementary release announcement for extensions and skins with security patches (1.31.15/1.35.3/1.36.1)**~~. 2021-06-21 21:18:52 (UTC+0)

Zabe claimed this task. 2021-06-22 10:03:58 (UTC+0)

> In ~~**T285190#7168051**~~, **@Mstyles** wrote:
> *@Zabe this patch works for globally suppressed users, but there are some users who have both `gu_status` and `lists` as attributes, in the database still have the same error message. Not sure if the patch should cover those users as well. Another patch can be submitted if that's the case. More context for hidden lists -> ⚓ https://phabricator.wikimedia.org/T192957*

Users with $mHidden set to 'lists' will be hidden on `Special:CentralAuth` and `Special:GlobalUsers`. Therefore I assume that they should also be hidden on `Special:GlobalUserRights`. So let me create a second patchset, which includes users with $mHidden set to 'lists'. On the other hand, I have to say that I don't know what you mean by `gu_status`.

Zabe added a project: **Patch-For-Review**. 2021-06-22 10:19:54 (UTC+0)

0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch 1 KB
Download

patchset 2

sbassett moved this task from **Our Part Is Done** to **Security Patch To Deploy** on the **Security-Team** board. 2021-06-22 15:23:34 (UTC+0)

sbassett added a subscriber: **sbassett**.

+1 to the patch above. We can try to get this updated patch out sometime this week during a train-friendly/backport window-friendly time.

sbassett triaged this task as *Low* priority. 2021-06-22 15:23:49 (UTC+0)

sbassett merged a task: ~~**T260863: Globally hidden usernames can be enumerated by unauthenticated users by crawling Special:GlobalUserRights with user IDs**~~. 2021-06-23 19:09:50 (UTC+0)

sbassett mentioned this in ~~**T260863: Globally hidden usernames can be enumerated by unauthenticated users by crawling Special:GlobalUserRights with user IDs**~~.

sbassett added a subscriber: **ST47**.

Mstyles added a comment. 2021-06-23 21:49:26 (UTC+0)

The patch was applied with .9 and .11 (https://sal.toolforge.org/log/VEzWOnoB1jz_IcWuA5fo), but this patch doesn't handle the user id scenario. This is mentioned in ~~T260863~~ which was merged into this ticket.

Zabe added a comment. 2021-06-23 21:51:08 (UTC+0)

> In ~~T285190#7173756~~, **@Mstyles** wrote:
> *This is mentioned in ~~T260863~~ which was merged into this ticket.*

Yeah, I can't see that one.

sbassett added a comment. 2021-06-23 22:09:08 (UTC+0)

@Zabe - @DannyS712 just subbed you to that task.

Zabe merged a task: ~~T260863: Globally hidden usernames can be enumerated by unauthenticated users by crawling Special:GlobalUserRights with user IDs~~. 2021-06-23 22:27:02 (UTC+0)

Zabe added a comment. Edited · 2021-06-23 22:34:59 (UTC+0)

0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch 1 KB
Download

patchset 3

This now includes a fix for the user id scenario described in ~~T260863~~. Sorry for me don't adding that in the previous one.

sbassett added a comment. Edited · 2021-06-24 14:24:31 (UTC+0)

> In ~~T285190#7173901~~, **@Zabe** wrote:
>
> ***0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch*** *1 KB*
> *Download*
>
> *patchset 3*

+1 to PS3. I feel like the logic could be condensed a bit more to be a bit more DRY, but this is fine for a security patch.

> *This now includes a fix for the user id scenario described in ~~T260863~~. Sorry for me don't adding that in the previous one.*

No problem, there are plenty of somewhat dated and forgotten bugs in Phab that deal with similar issues :) Given how long ~~T260863~~ was open, I think it can likely wait for deployment for next Monday's (2021-06-28) security window, unless anyone has more immediate concerns about it.

Zabe added a comment. 2021-06-29 21:27:02 (UTC+0)

I'm getting this on testwiki

```
[13f616c5-872f-4580-9947-57a0d6bfe4fc] /wiki/Special:GlobalUserRights?user=%2363654358 Error: Call to private CentralAuthGroupMembershipProxy::__construct() from context 'SpecialGlobalGroupMembership'

Backtrace:

from /srv/mediawiki/php-1.37.0-wmf.12/extensions/CentralAuth/includes/specials/SpecialGlobalGroupMembership.php(101)
#0 /srv/mediawiki/php-1.37.0-wmf.12/includes/specials/SpecialUserrights.php(141): SpecialGlobalGroupMembership->fetchUser(string, boolean)
#1 /srv/mediawiki/php-1.37.0-wmf.12/includes/specialpage/SpecialPage.php(646): UserrightsPage->execute(NULL)
#2 /srv/mediawiki/php-1.37.0-wmf.12/includes/specialpage/SpecialPageFactory.php(1362): SpecialPage->run(NULL)
#3 /srv/mediawiki/php-1.37.0-wmf.12/includes/MediaWiki.php(314): MediaWiki\SpecialPage\SpecialPageFactory->executePath(string, RequestContext)
#4 /srv/mediawiki/php-1.37.0-wmf.12/includes/MediaWiki.php(917): MediaWiki->performRequest()
#5 /srv/mediawiki/php-1.37.0-wmf.12/includes/MediaWiki.php(551): MediaWiki->main()
#6 /srv/mediawiki/php-1.37.0-wmf.12/index.php(53): MediaWiki->run()
#7 /srv/mediawiki/php-1.37.0-wmf.12/index.php(46): wfIndexMain()
#8 /srv/mediawiki/w/index.php(3): require(string)
#9 {main}
```

sbassett added a comment. 2021-06-29 21:31:17 (UTC+0)

@Zabe - yep, fixing with reverts right now.

Zabe added a comment. Edited · 2021-06-29 21:32:24 (UTC+0)

0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch 1 KB
Download

sorry, fixed the issue, if you haven't done that by your own already.

sbassett added a comment. 2021-06-29 21:34:28 (UTC+0)

> In ~~T285190#7185241~~, **@Zabe** wrote:
>
> ***0001-SECURITY-Act-like-users-don-t-exist-if-hidden-from-v.patch*** *1 KB*
> *Download*
>
> *sorry, fixed the issue, if you haven't done that by your own already.*

Ok, thanks. We'll pull to an mwdebug to test first this time.

sbassett added a comment. 2021-06-29 21:50:07 (UTC+0)

Ok, the buggy PS3 patch made it to wmf.11 and wmf.12 for a bit, but was reverted (1, 2). The new PS4 patch that fixed the bug was tested on mwdebug1002 and looked fine and was deployed to wmf.11 and wmf.12 (1, 2). We tested the enwiki link from ~~T260863~~ and there were no errors, and nothing in logstash either. So I think we're good for now.

sbassett moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board. 2021-06-29 21:58:13 (UTC+0)

sbassett changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2021-07-01 22:43:01 (UTC+0)

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

gerritbot added a comment. 2021-07-01 22:43:17 (UTC+0)

Change 702771 had a related patch set uploaded (by SBassett; author: Zabe):

[mediawiki/extensions/CentralAuth@master] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702771

gerritbot added a comment. 2021-07-01 22:43:47 (UTC+0)

Change 702722 had a related patch set uploaded (by SBassett; author: Zabe):

[mediawiki/extensions/CentralAuth@REL1_36] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702722

gerritbot added a comment. 2021-07-01 22:43:57 (UTC+0)

Change 702723 had a related patch set uploaded (by SBassett; author: Zabe):

[mediawiki/extensions/CentralAuth@REL1_35] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702723

gerritbot added a comment. 2021-07-01 22:44:06 (UTC+0)

Change 702724 had a related patch set uploaded (by SBassett; author: Zabe):

[mediawiki/extensions/CentralAuth@REL1_31] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702724

gerritbot added a comment. 2021-07-02 15:46:52 (UTC+0)

Change 702771 **merged** by jenkins-bot:

[mediawiki/extensions/CentralAuth@master] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702771

ReleaseTaggerBot added a project: ~~MW-1.37-notes (1.37.0-wmf.14; 2021-07-12)~~. 2021-07-02 16:00:19 (UTC+0)

gerritbot added a comment. 2021-07-02 16:06:20 (UTC+0)

Change 702724 **merged** by jenkins-bot:

[mediawiki/extensions/CentralAuth@REL1_31] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702724

gerritbot added a comment. 2021-07-02 16:08:10 (UTC+0)

Change 702723 **merged** by jenkins-bot:

[mediawiki/extensions/CentralAuth@REL1_35] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702723

gerritbot added a comment. 2021-07-02 16:11:01 (UTC+0)

Change 702722 **merged** by jenkins-bot:

[mediawiki/extensions/CentralAuth@REL1_36] SECURITY: Act like users don't exist if hidden from viewer

https://gerrit.wikimedia.org/r/702722

sbassett renamed this task from *Special:GlobalUserRights reveals existence of globally suppressed users* to *Special:GlobalUserRights reveals existence of globally suppressed users (CVE-2021-36127)*. 2021-07-02 20:04:23 (UTC+0)

sbassett closed this task as *Resolved*. 2021-07-02 20:16:11 (UTC+0)

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

CptViraj added a subscriber: **CptViraj**. 2021-07-03 17:01:28 (UTC+0)

Zabe removed a project: **Patch-For-Review**. 2021-07-15 15:46:29 (UTC+0)

Zabe mentioned this in ~~T290784: Security Issue Access Request for Zabe~~. 2022-01-10 23:00:08 (UTC+0)

Zabe removed a project: ~~User-Zabe~~. 2022-04-13 00:50:29 (UTC+0)