Maniphest › T276306

Create Task

CVE-2021-30156: Special:Contributions toolbar reveals existence of hidden users

Closed, Resolved   Public   SECURITY

Actions

Assigned To

taavi

Authored By

taavi
2021-03-03 10:05:02 (UTC+0)

Tags

Security-Team (Our Part Is Done)
Security
Vuln-Infoleak
MediaWiki-Blocks (Backlog)
MediaWiki-Special-pages (To triage)
User-Majavah (Done)
MW-1.37-notes (1.37.0-wmf.1; 2021-04-13)
MW-1.36-notes (Backlog)

Referenced Files

F34133819: T276306-PS1.patch
2021-03-03 10:46:27 (UTC+0)

F34133729: image.png
2021-03-03 10:05:02 (UTC+0)

F34133726: image.png
2021-03-03 10:05:02 (UTC+0)

Subscribers

Aklapper

Ammarpad

Bugreporter

DannyS712

gerritbot

Jdforrester-WMF

Reedy

View All 10 Subscribers

Description

Steps to reproduce

1. Using a suppressor account, completely block and suppress an user (User:Abusive username in my example), i.e. block talk page and emails, and select "Hide username from edits and lists"
2. While logged out, view `Special:Contributions/Abusive username`
3. Observe the toolbar at the top of the page.

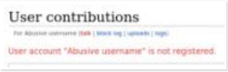
Expected results

1. The page does not show any indications that the account exists.

Actual results

1. Links to user talk, logs, etc, are shown, while they are not shown for non-existent users.

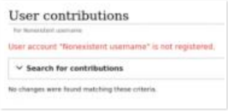
See screenshots:



User contributions

For Abusive username (talk | block log | uploads | logs)

User account "Abusive username" is not registered.



User contributions

For Nonexistent username

User account "Nonexistent username" is not registered.

Search for contributions

No changes were found matching these criteria.

Details

	Project	Subject
⚲	mediawiki/core	SECURITY: Do not reveal existence of hidden users in Special:Contribs
⚲	mediawiki/core	SECURITY: Do not reveal existence of hidden users in Special:Contribs

Customize query in gerrit

Related Objects

Mentions

Mentioned In
~~T285190: Special:GlobalUserRights reveals existence of globally suppressed users (CVE-2021-36127)~~
~~T270459: Tracking bug for MediaWiki 1.31.13/1.35.2~~

Mentioned Here
~~T211910: Don't show misleading messages on Special:Contributions for IP ranges outside the CIDR limit~~
rMW032dc91f4796: Don't show action links for IP ranges outside block limit
~~T270458: Release MediaWiki 1.31.13/1.35.2~~
rMWb5e7f210cd31: SECURITY: Act like users don't exist if hidden from viewer

taavi created this task. 2021-03-03 10:05:02 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-03-03 10:05:04 (UTC+0)

taavi added projects: **Vuln-Infoleak**, **MediaWiki-Blocks**, **MediaWiki-Special-pages**. 2021-03-03 10:08:49 (UTC+0)

taavi added a comment. 2021-03-03 10:13:47 (UTC+0)

Looks like this is related to {T120883}/CVE-2020-35480 which I can't see. This is still reproducible on master even when **b5e7f21** has been merged.

taavi added a project: **Patch-For-Review**. Edited · 2021-03-03 10:46:27 (UTC+0)

Turns out this was just a spot missed on that previous task. See attached patch set for a fix.

T276306-PS1.patch 1 KB
Download

Urbanecm added subscribers: **sbassett**, **Urbanecm**. 2021-03-03 12:42:35 (UTC+0)

Patch **approved** and deployed to both MW versions.

@sbassett Over to you to handle the final honors :).

sbassett added a parent task: ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-03-03 17:53:25 (UTC+0)

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. Edited · 2021-03-03 18:02:26 (UTC+0)
sbassett removed a project: **Patch-For-Review**.

Holding for the next security release (~~**T270458**~~) - please keep this task private for now. Also tracking as a current production security patch (T276237).

DannyS712 added a subscriber: **DannyS712**. 2021-03-03 23:18:01 (UTC+0)

Reedy mentioned this in ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-03-30 00:40:04 (UTC+0)

Reedy assigned this task to **taavi**. 2021-03-30 01:08:17 (UTC+0)

Restricted Application added a project: ~~**User-Majavah**~~. · View Herald Transcript 2021-03-30 01:08:20 (UTC+0)

taavi moved this task from **Unsorted** to **Done** on the ~~**User-Majavah**~~ board. 2021-03-30 09:15:38 (UTC+0)

Reedy added a subscriber: **Reedy**. 2021-04-04 23:06:22 (UTC+0)

Hmm. Does this apply to REL1_35/REL1_31?

It only looks like it applies to master, as it builds ontop of **rMW032dc91f4796: Don't show action links for IP ranges outside block limit** / ~~**T211910: Don't show misleading messages on Special:Contributions for IP ranges outside the CIDR limit**~~ which added the `$userObj->isRegistered()` check to the `if`

Reedy added a subscriber: **Ammarpad**. 2021-04-05 00:19:25 (UTC+0)

Reedy renamed this task from *Special:Contributions toolbar reveals existence of hidden users* to *CVE-2021-30156: Special:Contributions toolbar reveals existence of hidden users*. 2021-04-06 19:12:47 (UTC+0)

Jdforrester-WMF added a subscriber: **Jdforrester-WMF**. 2021-04-06 20:40:42 (UTC+0)

Looks to me like this is a prod-only one, so we can just push it into gerrit now.

Reedy removed a parent task: ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-04-06 20:43:09 (UTC+0)

taavi added a comment. 2021-04-06 21:00:49 (UTC+0)

Just tested with a REL1_35 install, the same issue is present even if it will need a modified patch due to changes in https://gerrit.wikimedia.org/r/c/mediawiki/core/+/589659.

Reedy added a parent task: ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-04-06 21:12:31 (UTC+0)

Reedy added a comment. 2021-04-06 21:28:07 (UTC+0)

> In ~~**T276306#6978045**~~, @Majavah wrote:
>
> *Just tested with a REL1_35 install, the same issue is present even if it will need a modified patch due to changes in https://gerrit.wikimedia.org/r/c/mediawiki/core/+/589659.*

Discussed on IRC... REL1_35 (and 1_31) just puts the sub heading on all talk pages. So there's nothing being disclosed in those versions. Vs what is there in master, which checks if it's a valid IP, or if the target user is registered. This is done without checking if the user doing the viewing has the permission to.

Will put it on gerrit

Reedy removed a parent task: ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-04-06 21:28:21 (UTC+0)

Reedy added a subscriber: **gerritbot**. 2021-04-06 21:37:04 (UTC+0)

gerritbot added a comment. 2021-04-06 22:05:59 (UTC+0)

Change 677370 **merged** by jenkins-bot:

[mediawiki/core@master] SECURITY: Do not reveal existence of hidden users in Special:Contribs

https://gerrit.wikimedia.org/r/677370

Reedy closed this task as *Resolved*. 2021-04-06 22:06:18 (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".

ReleaseTaggerBot added a project: ~~**MW-1.37-notes (1.37.0-wmf.1, 2021-04-13)**~~. 2021-04-06 23:00:21 (UTC+0)

gerritbot added a comment. 2021-04-08 20:59:39 (UTC+0)

Change 677960 had a related patch set uploaded (by Majavah; author: Majavah):

[mediawiki/core@REL1_36] SECURITY: Do not reveal existence of hidden users in Special:Contribs

https://gerrit.wikimedia.org/r/677960

gerritbot added a project: **Patch-For-Review**. 2021-04-08 20:59:40 (UTC+0)

Bugreporter added a subscriber: **Bugreporter**. 2021-04-08 22:42:34 (UTC+0)

There is another place that oversighted users are leaked (you can see my mention if you can see security tasks).

gerritbot added a comment. 2021-04-09 00:27:48 (UTC+0)

Change 677960 **merged** by jenkins-bot:

[mediawiki/core@REL1_36] SECURITY: Do not reveal existence of hidden users in Special:Contribs

https://gerrit.wikimedia.org/r/677960

ReleaseTaggerBot added a project: ~~**MW-1.36-notes**~~. 2021-04-09 01:00:37 (UTC+0)

Zabe mentioned this in ~~**T285190: Special:GlobalUserRights reveals existence of globally suppressed users (CVE-2021-36127)**~~. 2021-06-20 16:59:21 (UTC+0)

sbassett moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board. 2021-06-21 20:10:38 (UTC+0)

sbassett removed a project: **Patch-For-Review**.