Maniphest T418122 Create Task

CVE-2026-39937: Global vanishing does not remove the user email completely

Actions

Closed, Resolved Public SECURITY

Assigned To

M Mstyles

Authored By

U Urbanecm
2026-02-23 12:07:59 (UTC+0)

Tags

Security-Team (Watching)
Security
Account-Vanishing (Incoming)
MediaWiki-extensions-CentralAuth (Backlog)
Vuln-Infoleak
Essential-Work
MediaWiki-Platform-Team (Radar)
SecTeam-Processed (Completed)
Trust-and-Safety (Backlog)
Product Safety and Integrity (Sprint Forsythia (Mar 23 - Apr 10))) (Ready)

Referenced Files

F72291380: 01-T418122.patch
2026-02-23 13:52:14 (UTC+0)

Subscribers

A A09
Aklapper
Dragoniez
Dreamy_Jazz
gerritbot
Johannnes89
kostajh

View All 14 Subscribers

Description

When looking into a question raised by User:Cabayi in my mailbox, I noticed global account vanishing only removes the user email address from the `globaluser` record, but not from the (many) individual `user` tables. For example:

```
[urbanecm@stat1008 ~]$ analytics-mysql centralauth
mysql:research@dbstore1008.eqiad.wmnet [centralauth]> select gu_name, gu_email from globaluser where
gu_name='Renamed user 28145919bd97ab8be70d27c2e463c510';
+----------------------------------------------+----------+
| gu_name                                      | gu_email |
+----------------------------------------------+----------+
| Renamed user 28145919bd97ab8be70d27c2e463c510 |          |
+----------------------------------------------+----------+
1 row in set (0.001 sec)

mysql:research@dbstore1008.eqiad.wmnet [centralauth]> ^DBye
[urbanecm@stat1008 ~]$ analytics-mysql jawiki
mysql:research@dbstore1009.eqiad.wmnet [jawiki]> select user_name, user_email from user where
user_name='Renamed user 28145919bd97ab8be70d27c2e463c510';
+----------------------------------------------+----------------------------+
| user_name                                    | user_email                 |
+----------------------------------------------+----------------------------+
| Renamed user 28145919bd97ab8be70d27c2e463c510 | (REDACTED, CONTAINS USER EMAIL) |
+----------------------------------------------+----------------------------+
1 row in set (0.001 sec)

mysql:research@dbstore1009.eqiad.wmnet [jawiki]>
```

This is potentially significant, because we indicate emails are no longer kept. Also, IIRC, the feature was internalized into MediaWiki to be able to meet account deletion defined by Google/Apple.

Details

Author Affiliation
Wikimedia Communities

RELATED CHANGES IN GERRIT:

	Subject	Repo
	SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes	mediawiki/extensions/CentralAuth
	SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes	mediawiki/extensions/CentralAuth
	SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes	mediawiki/extensions/CentralAuth
	SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes	mediawiki/extensions/CentralAuth

Customize query in gerrit

Related Objects

Mentions

Mentioned In
T420848: AccountVanishing is marking endusers as system users
T421525: Should vanishing an account remove its password and other login credentials?
T411394: Write and send supplementary release announcement for extensions and skins with security patches (1.43.7/1.44.4/1.45.2)

Mentioned Here
T420848: AccountVanishing is marking endusers as system users
T421525: Should vanishing an account remove its password and other login credentials?
T104500: Old versions of sensitive user data (email, password hashes) can remain in database indefinitely due to local and global DB not being kept in sync

Urbanecm created this task. 2026-02-23 12:07:59 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2026-02-23 12:08:01 (UTC+0)

Urbanecm updated the task description. **(Show Details)** 2026-02-23 12:08:15 (UTC+0)

Urbanecm added projects: **Account-Vanishing**, **MediaWiki-extensions-CentralAuth**, **Product Safety and Integrity**.

Restricted Application added a project: **MediaWiki-Platform-Team**. · View Herald Transcript 2026-02-23 12:08:40 (UTC+0)

Urbanecm added a project: **Vuln-Infoleak**. 2026-02-23 12:10:21 (UTC+0)

Leaking only to shell holders, but..

This is the relevant piece of code from CentralAuth:

```
$data = [ 'gu_name' => $newname ];
if ( $type === GlobalRenameRequest::VANISH ) {
        // Vanish requests need to remove user's email
        $data[ 'gu_email' ] = '';
}
$dbw->newUpdateQueryBuilder()
        ->update( 'globaluser' )
        ->set( $data )
        ->where( [ 'gu_name' => $oldname ] )
        ->caller( __METHOD__ )
        ->execute();
```

Dreamy_Jazz triaged this task as *High* priority. 2026-02-23 12:27:49 (UTC+0)

taavi subscribed. 2026-02-23 13:35:24 (UTC+0)

(Partial) dupe of
T104500: Old versions of sensitive user data (email, password hashes) can remain in database indefinitely due to
?

kostajh subscribed. Edited · 2026-02-23 13:41:09 (UTC+0)

GlobalRenameUser::getJob doesn't access `$options['type']`, so the default parameter in LocalRenameUserJob (used for vanishing as well) is `GlobalRenameRequest::RENAME` when it should be `GlobalRenameRequest::VANISH`. That should be sufficient to address this, because then we'll hit the code path that uses `User::newSystemUser( $renamedUser->getName(), [ 'steal' => true ] );`

kostajh claimed this task. 2026-02-23 13:43:55 (UTC+0)

kostajh added a comment. 2026-02-23 13:52:14 (UTC+0)

01-T418122.patch 3 KB
Download

kostajh edited projects, added ~~**Product Safety and Integrity (Sprint Flower (Feb 9 - Feb 27))**~~, **Essential-Work**; removed **Product Safety and Integrity**. 2026-02-23 13:52:39 (UTC+0)

kostajh moved this task from **Backlog** to **Needs review** on the ~~**Product Safety and Integrity (Sprint Flower (Feb 9 - Feb 27))**~~ board.

Dreamy_Jazz subscribed. 2026-02-23 14:25:42 (UTC+0)

> In ~~**T418122#11640588**~~, @**kostajh** wrote:
>
> ***01-T418122.patch*** *3 KB*
> *Download*

LGTM, +2

Urbanecm added a comment. 2026-02-23 15:05:21 (UTC+0)

> In ~~**T418122#11640535**~~, @**kostajh** wrote:
>
> *GlobalRenameUser::getJob doesn't access `$options['type']`, so the default parameter in LocalRenameUserJob (used for vanishing as well) is `GlobalRenameRequest::RENAME` when it should be `GlobalRenameRequest::VANISH`. That should be sufficient to address this, because then we'll hit the code path that uses `User::newSystemUser( $renamedUser->getName(), [ 'steal' => true ] );`*

Note this has wider effects than email: It also scrubs `gu_password` and `user_password`, making the actions irreversible. FWIW, this came up in the context of https://meta.wikimedia.org/wiki/Talk:Account_vanishing#c-Cabayi-

20260223143200-Reversal_/_Unvanishing, where the reversibility is being discussed. (No objections towards deploying that though, I just want to make sure those consequences are known/expected in general)

kostajh added a comment. 2026-02-23 15:50:11 (UTC+0)

> In ~~T418122#11640803~~, @**Urbanecm** wrote:
>
> > In ~~T418122#11640535~~, @**kostajh** wrote:
> >
> > *GlobalRenameUser::getJob doesn't access `$options['type']`, so the default parameter in LocalRenameUserJob (used for vanishing as well) is `GlobalRenameRequest::RENAME` when it should be `GlobalRenameRequest::VANISH`. That should be sufficient to address this, because then we'll hit the code path that uses `User::newSystemUser( $renamedUser->getName(), [ 'steal' => true ] );`*
>
> *Note this has wider effects than email: It also scrubs `gu_password` and `user_password`, making the actions irreversible. FWIW, this came up in the context of https://meta.wikimedia.org/wiki/Talk:Account_vanishing#c-Cabayi-20260223143200-Reversal_/_Unvanishing, where the reversibility is being discussed. (No objections towards deploying that though, I just want to make sure those consequences are known/expected in general)*

I think that's OK, since that was already happening on the central wiki?

matmarex moved this task from **Inbox, needs triage** to **Radar** on the **MediaWiki-Platform-Team** board. 2026-02-23 15:50:28 (UTC+0)

matmarex edited projects, added **MediaWiki-Platform-Team (Radar)**; removed **MediaWiki-Platform-Team**.

sbassett subscribed. 2026-02-23 16:20:55 (UTC+0)

Are we still ok with the patch from ~~T418122#11640588~~? It seems reasonable to me. If folks are still ok with this approach for now, we could likely get this deployed during today's security deployment window.

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board. 2026-02-23 17:27:46 (UTC+0)

sbassett added a project: **SecTeam-Processed**.

sbassett added a project: **Trust-and-Safety**. 2026-02-23 17:31:05 (UTC+0)

• **Tgr** subscribed. 2026-02-23 18:11:56 (UTC+0)

The local password tables are empty on CentralAuth wikis anyway. The first system-user-ification will scrub the password from `globaluser`; that seems like a good thing from a privacy / data removal rights perspective.

kostajh added a comment. 2026-02-23 22:11:41 (UTC+0)

> In ~~T418122#11641296~~, @**sbassett** wrote:
>
> *Are we still ok with the patch from* ***~~T418122#11640588~~*** *? It seems reasonable to me. If folks are still ok with this approach for now, we could likely get this deployed during today's security deployment window.*

Yes, I think we should do it.

sbassett added a comment. 2026-02-23 23:08:20 (UTC+0)

Deployed to 1.46.0-wmf.16. Looks stable.

sbassett moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board. 2026-02-23 23:08:39 (UTC+0)

sbassett mentioned this in **T411394: Write and send supplementary release announcement for extensions and skins with security patches (1.43.7/1.44.4/1.45.2)**.

OKryva-WMF edited projects, added ~~**Product Safety and Integrity (Sprint Crocus (Mar 2 - Mar 20))**~~; removed ~~**Product Safety and Integrity (Sprint Flower (Feb 9 - Feb 27))**~~. 2026-03-02 16:33:58 (UTC+0)

OKryva-WMF moved this task from **Backlog** to **Needs review** on the ~~**Product Safety and Integrity (Sprint Crocus (Mar 2 - Mar 20))**~~ board. 2026-03-02 16:35:06 (UTC+0)

A09 subscribed. 2026-03-22 22:58:27 (UTC+0)

Johannnes89 subscribed. 2026-03-23 07:27:59 (UTC+0)

OKryva-WMF edited projects, added **Product Safety and Integrity (Sprint Forsythia (Mar 23 - Apr 10))**; removed ~~**Product Safety and Integrity (Sprint Crocus (Mar 2 - Mar 20))**~~. 2026-03-23 16:19:23 (UTC+0)

OKryva-WMF moved this task from **Backlog** to **Needs review** on the **Product Safety and Integrity (Sprint Forsythia (Mar 23 - Apr 10)))** board.

OKryva-WMF removed **kostajh** as the assignee of this task. 2026-03-24 13:01:25 (UTC+0)

OKryva-WMF moved this task from **Needs review** to **Ready** on the **Product Safety and Integrity (Sprint Forsythia (Mar 23 - Apr 10)))** board.

matmarex mentioned this in **T421525: Should vanishing an account remove its password and other login credentials?**. 2026-03-27 17:48:49 (UTC+0)

matmarex mentioned this in **T420848: AccountVanishing is marking endusers as system users**.

matmarex subscribed. 2026-03-27 17:53:35 (UTC+0)

This change caused vanished accounts to be labelled as "system users" in the wiki interface, e.g. on Special:UserRights, which was filed as **T420848: AccountVanishing is marking endusers as system users**. I was

quite confused what's happening until I found this task with its security patch.

A few people in that discussion pointed out that we had some ambiguous old decisions about *not* removing passwords from vanished users. I filed
T421525: Should vanishing an account remove its password and other login credentials? with a sketch of the history, so that we can once again and finally decide what should happen.

Reedy added a subscriber: **gerritbot**. 2026-04-01 13:02:32 (UTC+0)

Reedy subscribed.

Any objections for this patch to go through Gerrit?

sbassett added a comment. 2026-04-01 14:41:21 (UTC+0)

> In ~~**T418122#11777791**~~, @**Reedy** wrote:
>
> *Any objections for this patch to go through Gerrit?*

Not from me.

Change #1267098 had a related patch set uploaded (by Reedy; author: Kosta Harlan): 2026-04-02 15:51:29 (UTC+0)
[mediawiki/extensions/CentralAuth@master] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267098 **merged** by jenkins-bot: 2026-04-02 16:03:43 (UTC+0)
[mediawiki/extensions/CentralAuth@master] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267108 had a related patch set uploaded (by Reedy; author: Kosta Harlan): 2026-04-02 16:05:18 (UTC+0)
[mediawiki/extensions/CentralAuth@REL1_45] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267110 had a related patch set uploaded (by Reedy; author: Kosta Harlan): 2026-04-02 16:07:22 (UTC+0)
[mediawiki/extensions/CentralAuth@REL1_44] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267111 had a related patch set uploaded (by Reedy; author: Kosta Harlan): 2026-04-02 16:10:10 (UTC+0)
[mediawiki/extensions/CentralAuth@REL1_43] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267108 **merged** by jenkins-bot: 2026-04-02 16:25:33 (UTC+0)
[mediawiki/extensions/CentralAuth@REL1_45] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267110 **merged** by jenkins-bot: 2026-04-02 16:26:12 (UTC+0)
[mediawiki/extensions/CentralAuth@REL1_44] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes

Change #1267111 **merged** by jenkins-bot: [mediawiki/extensions/CentralAuth@REL1_43] SECURITY: Forward 'type' option to LocalRenameUserJob for vanishes 2026-04-02 16:41:13 (UTC+0)

Novem_Linguae subscribed. 2026-04-06 10:38:08 (UTC+0)

Mstyles renamed this task from *Global vanishing does not remove the user email completely* to *CVE-2026-39937: Global vanishing does not remove the user email completely*. 2026-04-07 22:28:24 (UTC+0)

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

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

Restricted Application added a subscriber: **Dragoniez**. · View Herald Transcript 2026-04-07 22:28:25 (UTC+0)

Mstyles closed this task as *Resolved*. 2026-04-07 22:31:07 (UTC+0)

Mstyles claimed this task.