

✓

Very long usernames can cause an infinite loop when loading Special:GlobalRenameRequest (CVE-2021-36125)

Actions

✓ Closed, Resolved

🌐 Public

SECURITY

Assigned To

Legoktm

Authored By

ST47  
2020-08-20 02:42:56 (UTC+0)

Tags

👤 Security-Team (Our Part Is Done)

👤 Security

👤 GlobalRename (Backlog)

👤 MediaWiki-extensions-CentralAuth (Incoming)

👤 Vuln-DoS (Tracked)

🔗 Patch-For-Review

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

Referenced Files

📄

F32189689: 0001-SECURITY-GlobalRename-Avoid-DoS-infinite-loop-in-sug.patch  
2020-08-20 08:16:48 (UTC+0)

Subscribers

Aklapper

bd808

• chasemp

Legoktm

RhinosF1

sbassett

ST47

View All 10 Subscribers

Description

Special:GlobalRenameRequest helpfully "suggests" a new username, which is the user's current username followed by three random characters:

```
do {  
    $rand = $this->getUser()->getName() . rand( 123, 999 );  
} while ( !GlobalRenameRequest::isNameAvailable( $rand )->isOk() );
```

If the user's current username is constructed such that none of those usernames can possibly pass `isNameAvailable`, this will loop forever. Presumably, this consumes 100% of a CPU core until the request times out.

I considered registering all of `User:ST47123 .. User:ST47999`, but I'm lazy and there is an easier way.

The new username must pass [all of the tests in `UserNameUtils.php`](#), including that the new username must not be longer than `MaxNameChars` (which is 85 on WMF). If the current username is at least 83 characters long, this will loop forever. With sufficient threads, this could very easily DoS the site.

I would suggest removing this "suggested username" feature from `GlobalRenameRequest` entirely, as adding three digits to the end of the username isn't a very good suggestion anyway.

If a traceback would be helpful, you can find one here: `[fc0657b2-77c2-41eb-9996-ce38f062394a] 2020-08-20 02:27:10: Fatal exception of type "WMFTimeoutException"`

Details

Author Affiliation

Wikimedia Communities

Project	Subject
<a href="#">mediawiki/extensions/CentralAuth</a>	SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature
<a href="#">mediawiki/extensions/CentralAuth</a>	SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature
<a href="#">mediawiki/extensions/CentralAuth</a>	SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature

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

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

Legoktm added a project: **GlobalRename**. 2020-08-20 08:03:15 (UTC+0)

Legoktm added a subscriber: **Legoktm**.

I think the easiest fix is to just add a counter and stop after say 5 tries.

...as adding three digits to the end of the username isn't a very good suggestion anyway.

Why not?

Restricted Application added a project: **MediaWiki-extensions-CentralAuth**. · View Herald Transcript 2020-08-20 08:03:16 (UTC+0)

Legoktm added projects: **Patch-For-Review**, **Vuln-DoS**. 2020-08-20 08:16:48 (UTC+0)

Legoktm added a subscriber: **bd808**.

Here's a quick patch:

**0001-SECURITY-GlobalRename-Avoid-DoS-infinite-loop-in-sug.patch** 4 KB

Download

chasemp added a subscriber: **chasemp**. 2020-08-20 11:10:20 (UTC+0)

Urbanecm triaged this task as *High* priority. 2020-08-20 11:51:32 (UTC+0)

ST47 added a comment. 2020-08-20 16:51:05 (UTC+0)

In **T260865#6398926**, @Legoktm wrote:

...as adding three digits to the end of the username isn't a very good suggestion anyway.

Why not?

It doesn't really matter, but if someone is going to request a global rename, their intent is probably not to just add a few digits to the end of their current name. I think most global renames are done either to correct problems with a project's username policy (such as usernames that represent a company), or to remove someone's real name from their username, which "just stick 123 on the end" doesn't really help with.

bd808 added a comment. 2020-08-20 17:48:34 (UTC+0)

In **T260865#6398950**, @Legoktm wrote:

Here's a quick patch:

**0001-SECURITY-GlobalRename-Avoid-DoS-infinite-loop-in-sug.patch** 4 KB

Download

LGTM. I should be trouted for writing that original loop.

bd808 added a comment. 2020-08-20 17:49:03 (UTC+0)

In **T260865#6400504**, @ST47 wrote:

It doesn't really matter, but if someone is going to request a global rename, their intent is probably not to just add a few digits to the end of their current name.

This logic is from the time of SUL unification and the "add a random suffix" bit was mostly about making things slightly easier for folks who "lost" their local username due to unification. I think I would agree that it is of low value in any wiki farm that did not have a unification step to pass through. And it should be mostly useless today in the Wikimedia farm. Which I guess is a long way of saying I would not be personally sad for the fix to be a simpler version of [@Legoktm](#)'s patch that just drops the suggestion part entirely.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2020-08-24 15:20:36 (UTC+0)

Aklapper added a comment. 2020-09-18 15:21:19 (UTC+0)

In **T260865#6400643**, @bd808 wrote:

I would not be personally sad for the fix to be a simpler version of [@Legoktm](#)'s patch that just drops the suggestion part entirely.

Any opinions whether to simplify the patch, and/or anyone willing to get that patch merged?

sbassett moved this task from **Watching** to **Security Patch To Deploy** on the **Security-Team** board. 2021-03-25 15:46:38 (UTC+0)

sbassett added a subscriber: **sbassett**. 2021-05-17 21:49:02 (UTC+0)

Rebased and **deployed** the above security patch (**T260865#6398950**) to wmf.5. Logs seems fine. Will also track at **T279733**.

sbassett moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board. 2021-05-17 21:49:23 (UTC+0)

sbassett mentioned this in **T279733**: **Write and send supplementary release announcement for extensions and skins with security patches (1.34.15/1.35.3/1.36.1)**.

sbassett lowered the priority of this task from *High* to *Low*. 2021-07-01 21:51:46 (UTC+0)

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




















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

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 21:52:05 (UTC+0)

Change 702757 had a related patch set uploaded (by SBassett; author: SBassett):  
  
[mediawiki/extensions/CentralAuth@master] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature

<a href="https:// Gerrit.wikimedia.org/r/702757">https:// Gerrit.wikimedia.org/r/702757</a>	
 <b>gerritbot</b> added a project: <b>Patch-For-Review</b> . 2021-07-01 21:52:05 (UTC+0)	
Change 702715 had a related patch set uploaded (by SBassett; author: SBassett):  [mediawiki/extensions/CentralAuth@REL1_36] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature  <a href="https:// Gerrit.wikimedia.org/r/702715">https:// Gerrit.wikimedia.org/r/702715</a>	
 <b>gerritbot</b> added a comment. 2021-07-01 21:53:03 (UTC+0)	
Change 702716 had a related patch set uploaded (by SBassett; author: SBassett):  [mediawiki/extensions/CentralAuth@REL1_35] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature  <a href="https:// Gerrit.wikimedia.org/r/702716">https:// Gerrit.wikimedia.org/r/702716</a>	
 <b>RhinosF1</b> added a subscriber: <b>RhinosF1</b> . 2021-07-01 21:53:10 (UTC+0)	
 <b>Zabe</b> added a subscriber: <b>Zabe</b> . 2021-07-01 22:32:07 (UTC+0)	
 <b>Universal_Omega</b> added a subscriber: <b>Universal_Omega</b> . 2021-07-01 23:44:17 (UTC+0)	
 <b>valerio.bozzolan</b> added a subscriber: <b>valerio.bozzolan</b> . 2021-07-02 11:57:18 (UTC+0)	
 <b>gerritbot</b> added a comment. 2021-07-02 15:47:06 (UTC+0)	
Change 702757 <b>merged</b> by jenkins-bot:  [mediawiki/extensions/CentralAuth@master] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature  <a href="https:// Gerrit.wikimedia.org/r/702757">https:// Gerrit.wikimedia.org/r/702757</a>	
 <b>ReleaseTaggerBot</b> added a project: <del><b>MW-1.37-notes (1.37.0 wmf.14; 2021-07-12)</b></del> . 2021-07-02 16:00:15 (UTC+0)	
 <b>gerritbot</b> added a comment. 2021-07-02 16:12:44 (UTC+0)	
Change 702716 <b>merged</b> by jenkins-bot:  [mediawiki/extensions/CentralAuth@REL1_35] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature  <a href="https:// Gerrit.wikimedia.org/r/702716">https:// Gerrit.wikimedia.org/r/702716</a>	
 <b>gerritbot</b> added a comment. 2021-07-02 16:12:59 (UTC+0)	
Change 702715 <b>merged</b> by jenkins-bot:  [mediawiki/extensions/CentralAuth@REL1_36] SECURITY: GlobalRename: Avoid DoS/infinite loop in suggested username feature  <a href="https:// Gerrit.wikimedia.org/r/702715">https:// Gerrit.wikimedia.org/r/702715</a>	
 <b>sbassett</b> renamed this task from <i>Very long usernames can cause an infinite loop when loading Special:GlobalRenameRequest</i> to <i>Very long usernames can cause an infinite loop when loading Special:GlobalRenameRequest (CVE-2021-36125)</i> . 2021-07-02 20:01:22 (UTC+0)	
 <b>sbassett</b> closed this task as <i>Resolved</i> . 2021-07-02 20:10:34 (UTC+0)	
 <b>sbassett</b> assigned this task to <b>Legoktm</b> .	
 <b>sbassett</b> moved this task from <b>Watching to Our Part Is Done</b> on the <b>Security-Team</b> board.	