☑ CVE-2022-28203: Requesting Special:NewFiles in commons with actor as a condition can bring the whole database down

☰ Actions

☑ Closed, Resolved Public SECURITY

Assigned To

Ladsgroup

Authored By

Ladsgroup
2021-12-14 17:57:59 (UTC+0)

Tags

Security-Team (Watching)

Security

DBA (Done)

User-Ladsgroup (Done)

Performance Issue

SecTeam-Processed (Completed)

Referenced Files

F34883919: T297731.patch
2021-12-14 18:22:39 (UTC+0)

Subscribers

Aklapper

daniel

gerritbot

Jdforrester-WMF

Krinkle

Ladsgroup

LSobanski

View All 12 Subscribers

Description

I have been seeing a lot of slow queries like this:

```
wikiadmin@10.64.16.175(commonswiki)> explain SELECT  /*! STRAIGHT_JOIN */
img_name,img_timestamp,actor_user,actor_name  FROM `image` JOIN `actor` ON ((actor_id=img_actor))
LEFT JOIN `user_groups` ON (ug_group = 'bot' AND (ug_user = actor_user) AND (ug_expiry IS NULL OR
ug_expiry >= '20211214173620'))   WHERE actor_name = 'Gov.mm' AND (ug_group IS NULL) AND
(((img_timestamp<'20211214000000')))  ORDER BY img_timestamp DESC LIMIT 51  ;
+------+-------------+-------------+--------+------------------------------------+---------------+----
-----+-------------------------------------+----------+------------------------+
| id   | select_type | table       | type   | possible_keys                      | key           |
key_len | ref                               | rows     | Extra                  |
+------+-------------+-------------+--------+------------------------------------+---------------+----
-----+-------------------------------------+----------+------------------------+
|    1 | SIMPLE      | image       | range  | img_timestamp,img_actor_timestamp | img_timestamp | 14
| NULL                              | 29263285 | Using where            |
|    1 | SIMPLE      | actor       | const  | PRIMARY,actor_name                 | actor_name    | 257
| const                             | 1        | Using where            |
|    1 | SIMPLE      | user_groups | eq_ref | PRIMARY,ug_group,ug_expiry         | PRIMARY       | 261
| commonswiki.actor.actor_user,const | 1        | Using where; Not exists |
+------+-------------+-------------+--------+------------------------------------+---------------+----
-----+-------------------------------------+----------+------------------------+
3 rows in set (0.004 sec)
```

The straight join is actually problematic, if you remove it, MySQL realizes the user doesn't exists and return with empty result right away:

```
wikiadmin@10.64.16.175(commonswiki)> explain SELECT  img_name,img_timestamp,actor_user,actor_name
FROM `image` JOIN `actor` ON ((actor_id=img_actor)) LEFT JOIN `user_groups` ON (ug_group = 'bot' AND
(ug_user = actor_user) AND (ug_expiry IS NULL OR ug_expiry >= '20211214173620'))   WHERE actor_name =
'Gov.mm' AND (ug_group IS NULL) AND (((img_timestamp<'20211214000000')))  ORDER BY img_timestamp DESC
LIMIT 51  ;
+------+-------------+-------+------+---------------+------+---------+------+------+-----------------
-----------------------------------+
| id   | select_type | table | type | possible_keys | key  | key_len | ref  | rows | Extra
|
+------+-------------+-------+------+---------------+------+---------+------+------+-----------------
-----------------------------------+
|    1 | SIMPLE      | NULL  | NULL | NULL          | NULL | NULL    | NULL | NULL | Impossible WHERE
noticed after reading const tables |
+------+-------------+-------+------+---------------+------+---------+------+------+-----------------
-----------------------------------+
1 row in set (0.001 sec)

wikiadmin@10.64.16.175(commonswiki)> SELECT  img_name,img_timestamp,actor_user,actor_name  FROM
`image` JOIN `actor` ON ((actor_id=img_actor)) LEFT JOIN `user_groups` ON (ug_group = 'bot' AND
(ug_user = actor_user) AND (ug_expiry IS NULL OR ug_expiry >= '20211214173620'))   WHERE actor_name =
'Gov.mm' AND (ug_group IS NULL) AND (((img_timestamp<'20211214000000')))  ORDER BY img_timestamp DESC
LIMIT 51  ;
Empty set (0.001 sec)
```

You can replace "Gov.mm" with any gibberish and it would still goes in direction of reading 29M rows. Suggestion: Just run a check if the actor exists before making the query.

Details

	Project	Subject
⑂	mediawiki/core	SECURITY: pagers: Don't make a straight join if the user is set

mediawiki/core SECURITY: pagers: Don't make a straight join if the user is set

mediawiki/core SECURITY: pagers: Don't make a straight join if the user is set

mediawiki/core SECURITY: pagers: Don't make a straight join if the user is set

mediawiki/core SECURITY: pagers: Don't make a straight join if the user is set

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

	Status	Assigned	Task
	☑ Resolved	Reedy	**~~T297829~~ Release MediaWiki 1.35.6/1.36.4/1.37.2**
⌃	☑ Resolved	Reedy	**~~T297830~~ Tracking bug for MediaWiki 1.35.6/1.36.4/1.37.2**
	☑ Resolved	Ladsgroup	**~~T297731~~ CVE-2022-28203: Requesting Special:NewFiles in commons with actor a...**

Ladsgroup created this task. 2021-12-14 17:57:59 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-12-14 17:58:00 (UTC+0)

Ladsgroup added a comment. 2021-12-14 18:01:12 (UTC+0)

It is the same with existing actors too:

```
wikiadmin@10.64.16.175(commonswiki)> explain SELECT  /*! STRAIGHT_JOIN */
img_name,img_timestamp,actor_user,actor_name  FROM `image` JOIN `actor` ON ((actor_id=img_actor))
LEFT JOIN `user_groups` ON (ug_group = 'bot' AND (ug_user = actor_user) AND (ug_expiry IS NULL OR
ug_expiry >= '20211214173620'))   WHERE actor_name = 'Ladsgroup' AND (ug_group IS NULL) AND
(((img_timestamp<'20211214000000')))  ORDER BY img_timestamp DESC LIMIT 51  ;
+------+-------------+-------------+--------+------------------------------------+---------------+---
------+-----------------------------------+----------+------------------------+
| id   | select_type | table       | type   | possible_keys                      | key           |
key_len | ref                             | rows     | Extra                  |
+------+-------------+-------------+--------+------------------------------------+---------------+---
------+-----------------------------------+----------+------------------------+
|    1 | SIMPLE      | image       | range  | img_timestamp,img_actor_timestamp | img_timestamp | 14
| NULL                              | 29263338 | Using where            |
|    1 | SIMPLE      | actor       | const  | PRIMARY,actor_name                 | actor_name    |
257     | const                           | 1        | Using where            |
|    1 | SIMPLE      | user_groups | eq_ref | PRIMARY,ug_group,ug_expiry         | PRIMARY       |
261     | commonswiki.actor.actor_user,const | 1        | Using where; Not exists |
+------+-------------+-------------+--------+------------------------------------+---------------+---
------+-----------------------------------+----------+------------------------+
3 rows in set (0.001 sec)
```

While without STRAIGHT_JOIN it's much faster:

```
wikiadmin@10.64.16.175(commonswiki)> explain SELECT img_name,img_timestamp,actor_user,actor_name
FROM `image` JOIN `actor` ON ((actor_id=img_actor)) LEFT JOIN `user_groups` ON (ug_group = 'bot' AND
(ug_user = actor_user) AND (ug_expiry IS NULL OR ug_expiry >= '20211214173620'))   WHERE actor_name
= 'Ladsgroup' AND (ug_group IS NULL) AND (((img_timestamp<'20211214000000')))  ORDER BY
img_timestamp DESC LIMIT 51  ;
+------+-------------+-------------+-------+------------------------------------+--------------------
-+---------+-------------+------+-------------------------+
| id   | select_type | table       | type  | possible_keys                      | key
| key_len | ref         | rows | Extra                   |
+------+-------------+-------------+-------+------------------------------------+--------------------
-+---------+-------------+------+-------------------------+
|    1 | SIMPLE      | actor       | const | PRIMARY,actor_name                 | actor_name
| 257     | const       | 1    |                         |
|    1 | SIMPLE      | user_groups | const | PRIMARY,ug_group,ug_expiry         | PRIMARY
| 261     | const,const | 0    | Unique row not found    |
|    1 | SIMPLE      | image       | range | img_timestamp,img_actor_timestamp | img_actor_timestamp
| 22      | NULL        | 395  | Using where; Using index |
+------+-------------+-------------+-------+------------------------------------+--------------------
-+---------+-------------+------+-------------------------+
3 rows in set (0.003 sec)
```

Ladsgroup claimed this task. 2021-12-14 18:02:23 (UTC+0)

Ladsgroup triaged this task as *High* priority.

Ladsgroup added a project: **DBA**.

Restricted Application added a project: ~~User-Ladsgroup~~. · View Herald Transcript 2021-12-14 18:02:24 (UTC+0)

Ladsgroup moved this task from **Triage** to **In progress** on the **DBA** board. 2021-12-14 18:02:36 (UTC+0)

Ladsgroup added a comment. 2021-12-14 18:04:51 (UTC+0)

It needs a simple join decomposition. I will never understand the fascination of mediawiki with join. Each purge makes around 200 queries with warm cache and 1k with cold one and we are worried about one more really fast query, it's not making them across the Atlantic ocean, the network latency is small.

Ladsgroup added subscribers: **tstarling**, **Krinkle**, **daniel**, • **Pchelolo**. 2021-12-14 18:22:39 (UTC+0)

Here is the fix. I think we need to roll this out to all pagers that set the user and do straight join but that's for later. I appreciate code review on this.

T297731.patch 1 KB
Download

Marostegui added a comment. 2021-12-14 18:30:28 (UTC+0)

It would be nice to roll this out this week before the code freeze - great catch Amir!

Ladsgroup renamed this task from *Requesting Special:NewFiles in commons with non-existentant actors can bring the whole database down* to *Requesting Special:NewFiles in commons with actor as a condition can bring the whole* *database down* . 2021-12-14 18:49:25 (UTC+0)

Jdforrester-WMF added a subscriber: **Jdforrester-WMF**. Edited · 2021-12-14 18:50:33 (UTC+0)

> In **~~T297731#7570609~~**, **@Ladsgroup** wrote:
>
> *Here is the fix. I think we need to roll this out to all pagers that set the user and do straight join but that's for later. I appreciate code review on this.*
>
> ***T297731.patch*** *1 KB*
> *Download*

That seems fine for now, yes. C+2.

Reedy added a project: **Performance Issue**. 2021-12-15 11:43:14 (UTC+0)

Ladsgroup added a comment. 2021-12-15 16:41:38 (UTC+0)

This is deployed now.

Ladsgroup added a comment. 2021-12-15 16:45:32 (UTC+0)

We should monitor https://logstash.wikimedia.org/goto/7d3662149d8277dd9a9574c833b41163 to see if it's fully stopped.

sbassett added a subscriber: **sbassett**. 2021-12-15 21:56:05 (UTC+0)

Thanks for the deploy, **@Ladsgroup**. Now tracked at T276237 and will eventually be part of the *next* security release, due out around the end of March 2022.

Ladsgroup moved this task from **In progress** to **Done** on the **DBA** board. 2021-12-16 11:11:10 (UTC+0)

> In **~~T297731#7572893~~**, **@Ladsgroup** wrote:
>
> *We should monitor https://logstash.wikimedia.org/goto/7d3662149d8277dd9a9574c833b41163 to see if it's fully stopped.*

Log is clean. I move this to done but won't close it so it gets properly processed by security team.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2021-12-20 16:34:16 (UTC+0)

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

Ladsgroup closed this task as *Resolved*. 2021-12-21 09:16:26 (UTC+0)

Log is fully cleaned up. This is done.

sbassett added a parent task: ~~**T297830: Tracking bug for MediaWiki 1.35.6/1.36.4/1.37.2**~~.
2021-12-21 15:37:21 (UTC+0)

Reedy mentioned this in ~~**T297830: Tracking bug for MediaWiki 1.35.6/1.36.4/1.37.2**~~. 2022-03-20 12:46:10 (UTC+0)

Reedy added a subscriber: **gerritbot**. 2022-03-28 13:32:31 (UTC+0)

Reedy renamed this task from *Requesting Special:NewFiles in commons with actor as a condition can bring the whole database down* to *CVE-2022-: Requesting Special:NewFiles in commons with actor as a condition can bring the whole database down* . 2022-03-28 13:52:49 (UTC+0)

Reedy mentioned this in ~~**T297831: Obtain CVEs for 1.35.6/1.36.4/1.37.2 security releases**~~.

Reedy renamed this task from *CVE-2022-: Requesting Special:NewFiles in commons with actor as a condition can bring the whole database down* to *CVE-2022-28203: Requesting Special:NewFiles in commons with actor as a condition can bring the whole database down* . 2022-03-30 18:03:20 (UTC+0)

gerritbot added a comment. 2022-03-31 21:43:47 (UTC+0)

Change 775972 had a related patch set uploaded (by Reedy; author: Amir Sarabadani):

[mediawiki/core@REL1_35] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775972

gerritbot added a project: **Patch-For-Review**. 2022-03-31 21:43:49 (UTC+0)

gerritbot added a comment. 2022-03-31 21:53:43 (UTC+0)

Change 775972 **merged** by jenkins-bot:

[mediawiki/core@REL1_35] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775972

gerritbot added a comment. 2022-03-31 21:56:30 (UTC+0)

Change 775977 had a related patch set uploaded (by Reedy; author: Amir Sarabadani):

[mediawiki/core@REL1_36] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775977

gerritbot added a comment. 2022-03-31 22:07:08 (UTC+0)

Change 775983 had a related patch set uploaded (by Reedy; author: Amir Sarabadani):

[mediawiki/core@REL1_37] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775983

gerritbot added a comment. 2022-03-31 22:08:11 (UTC+0)

Change 775977 **merged** by jenkins-bot:

[mediawiki/core@REL1_36] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775977

gerritbot added a comment. 2022-03-31 22:19:42 (UTC+0)

Change 775983 **merged** by jenkins-bot:

[mediawiki/core@REL1_37] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775983

gerritbot added a comment. 2022-03-31 22:19:45 (UTC+0)

Change 775991 had a related patch set uploaded (by Reedy; author: Amir Sarabadani):

[mediawiki/core@master] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775991

gerritbot added a comment. 2022-03-31 22:21:05 (UTC+0)

Change 775994 had a related patch set uploaded (by Reedy; author: Amir Sarabadani):

[mediawiki/core@REL1_38] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775994

gerritbot added a comment. 2022-03-31 22:34:53 (UTC+0)

Change 775994 **merged** by jenkins-bot:

[mediawiki/core@REL1_38] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775994

gerritbot added a comment. 2022-03-31 22:39:33 (UTC+0)

Change 775991 **merged** by jenkins-bot:

[mediawiki/core@master] SECURITY: pagers: Don't make a straight join if the user is set

https://gerrit.wikimedia.org/r/775991

Reedy changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2022-03-31 23:05:08 (UTC+0)

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

Maintenance_bot removed a project: **Patch-For-Review**. 2022-03-31 23:10:21 (UTC+0)

Zabe added a subscriber: **Zabe**. 2022-03-31 23:12:20 (UTC+0)

Maintenance_bot moved this task from **Incoming** to **Done** on the ~~**User-Ladsgroup**~~ board.

2022-03-31 23:15:23 (UTC+0)