Maniphest T418222 Create Task

CVE-2026-39934: With hidden mentees, ReassignMenteesJob runs as an infinite loop

Actions

Closed, Resolved Public SECURITY

Assigned To

U Urbanecm_WMF

Authored By

U Urbanecm_WMF
2026-02-24 11:04:03 (UTC+0)

Tags

GrowthExperiments-Mentorship (New Tasks)

Security

Security-Team (Watching)

MW-1.46-notes (1.46.0-wmf.17; 2026-02-24)

SecTeam-Processed (Completed)

Growth-Team (FY2025-26 Q3 Sprint 5) (Test in Production)

Referenced Files

F72317056: T418222.patch
2026-02-24 16:54:31 (UTC+0)

Subscribers

A A_smart_kitten

Aklapper

ASanford-WMF

Cyndymediawiksim

DMburugu

EMcFarland-WMF

Etonkovidova

View All 15 Subscribers

Description

I discovered `ReassignMenteesJob` runs over a thousand times per day for one cswiki former mentee:

```
[urbanecm@mwlog2002 /srv/mw-log]$ grep ReassignMenteesJob archive/GrowthExperiments.log-20260224 |
grep Felix220  | wc -l
1434
[urbanecm@mwlog2002 /srv/mw-log]$ zgrep ReassignMenteesJob archive/GrowthExperiments.log-20260223.gz
| grep Felix220  | wc -l
1426
[urbanecm@mwlog2002 /srv/mw-log]$
```

despite the mentor resigned over a month ago. The job is continuously rescheduled by the mechanism added in ~~**T354222: reassignMenteesJob is not able to finish in time when a mentor has too many mentees assigned**~~:

```
2026-02-23 01:17:59.041757 [9aa82291-b683-49b0-b4f1-0ea8f9900835] mw-jobrunner.codfw.main-
546746cf89-x62xw cswiki 1.46.0-wmf.16 GrowthExperiments INFO:
GrowthExperiments\Mentorship\ReassignMentees::doReassignMentees processing 0 mentees
{"mentees":0,"context.job_type":"reassignMenteesJob"}
2026-02-23 01:17:59.042473 [9aa82291-b683-49b0-b4f1-0ea8f9900835] mw-jobrunner.codfw.main-
546746cf89-x62xw cswiki 1.46.0-wmf.16 GrowthExperiments INFO: ReassignMenteesJob finished
reassignment with 1 status {"status":true,"context.job_type":"reassignMenteesJob"}
2026-02-23 01:17:59.043524 [9aa82291-b683-49b0-b4f1-0ea8f9900835] mw-jobrunner.codfw.main-
546746cf89-x62xw cswiki 1.46.0-wmf.16 GrowthExperiments INFO: ReassignMenteesJob did not reassign
all mentees, scheduling new job {"mentor":"Felix220","context.job_type":"reassignMenteesJob"}
```

despite there being zero mentees to process.

What is happening is this:

1. The mentor resigned, `ReassignMenteesJob` fires for the first time. It reassigns the mentees to someone else (logs)
2. Once the reassignment finishes, the job checks `MentorStore::hasAnyMentees()` to see whether there are any mentees remaining (cf. ~~**T354222**~~ for why this was added)
3. `MentorStore::hasAnyMentees()` checks for *all* mentees (including mentees whose accounts were hidden by an oversighter). Felix220 does have one hidden mentee, so this method returns true.
4. `ReassignMenteesJob` fires again. It calls `MentorStore::getMenteesByMentor()` to find the list of mentees. By default, `MentorStore::getMenteesByMentor` _ignores_ hidden mentees. For Felix220, it returns an empty array.
5. The job doesn't do anything and it returns successfully
6. We go back to step 2, and the process repeats...infinitely

This is happening since r1077077: MentorStore::hasAnyMentees: Use more efficient implementation (~~**T376124**~~), which we merged in 2024 (!), which removed the exclusion of hidden users in `MentorStore::hasAnyMentees()`.

WMF-NDA queries confirming the above findings:

{P89004}

Details

RELATED CHANGES IN GERRIT:

Subject	Repo

	SECURITY: ReassignMentees: Handle hidden users correctly	mediawiki/extensions/GrowthExperiments
	SECURITY: ReassignMentees: Handle hidden users correctly	mediawiki/extensions/GrowthExperiments
	SECURITY: ReassignMentees: Handle hidden users correctly	mediawiki/extensions/GrowthExperiments

Customize query in gerrit

Related Objects

Mentions

Mentioned In
T411394: Write and send supplementary release announcement for extensions and skins with security patches (1.43.7/1.44.4/1.45.2)
T418194: Mentors still having mentees after removing themselves

Mentioned Here
T411394: Write and send supplementary release announcement for extensions and skins with security patches (1.43.7/1.44.4/1.45.2)
~~T354222: reassignMenteesJob is not able to finish in time when a mentor has too many mentees assigned~~
~~T376124: Removing a mentor from the list of mentors does not always reassign newcomers~~

Urbanecm_WMF created this task. 2026-02-24 11:04:03 (UTC+0)

Restricted Application added a project: **Growth-Team**. · View Herald Transcript 2026-02-24 11:04:04 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript

Urbanecm_WMF updated the task description. **(Show Details)** 2026-02-24 11:07:04 (UTC+0)

Michael subscribed. 2026-02-24 11:10:05 (UTC+0)

Michael changed the visibility from "Public (No Login Required)" to "Subscribers". 2026-02-24 11:12:42 (UTC+0)

Michael changed the edit policy from "All Users" to "Subscribers".

Urbanecm_WMF changed the visibility from "Subscribers" to "**Custom Policy**". 2026-02-24 11:19:06 (UTC+0)

Urbanecm_WMF changed the edit policy from "Subscribers" to "**Custom Policy**".

Urbanecm changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2026-02-24 11:19:57 (UTC+0)

Urbanecm set Security to Software security bug.

Urbanecm added projects: **Security**, **Security-Team**.

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

Urbanecm changed the subtype of this task from "Task" to "Security Issue".

Urbanecm subscribed.

Restricted Application removed a subscriber: **Urbanecm**. · View Herald Transcript 2026-02-24 11:20:06 (UTC+0)

Urbanecm_WMF claimed this task. 2026-02-24 13:45:47 (UTC+0)

Urbanecm_WMF triaged this task as *High* priority.

Urbanecm_WMF edited projects, added ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~; removed **Growth-Team**.

Urbanecm_WMF added subscribers: **Etonkovidova**, **EMcFarland-WMF**, **Cyndymediawiksim** and **4 others**.

Urbanecm_WMF mentioned this in **T418194: Mentors still having mentees after removing themselves**.
2026-02-24 16:48:37 (UTC+0)

Urbanecm_WMF added a comment. 2026-02-24 16:54:31 (UTC+0)

Fix attached

T418222.patch 8 KB
Download

The fix needs to be applied on top of r1243136 to ensure a clear application.

Urbanecm_WMF moved this task from **Incoming** to **Code Review** on the ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~ board. 2026-02-24 16:59:29 (UTC+0)

Michael added a comment. 2026-02-25 14:52:08 (UTC+0)

> In ~~**T418222#11647157**~~, **@Urbanecm_WMF** wrote:
>
> *Fix attached*
>
> ***T418222.patch*** *8 KB*
> *Download*
>
> *The fix needs to be applied on top of r1243136 to ensure a clear application.*

This looks sensible to me. I give it my virtual +2

Urbanecm_WMF moved this task from **Code Review** to **Doing** on the ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~ board. 2026-02-25 15:04:31 (UTC+0)

Thanks! Moving to Doing, I'll deploy it soon.

Urbanecm_WMF added a comment. 2026-02-25 15:25:59 (UTC+0)

This is not the easiest patch to deploy... To be able to deploy it w/o merge conflicts, we need to pull a bunch of code refactors to production... Here is a list of patches to backport to wmf.16:

```
095f9d41a79f5678bcd712b3381b6c687b2498b5 (Sergio, geForceVariant)
7d8940d87cbce001ac836ca78e4f9e27192a9a63 (SiteNotice)
d7c8e88419b102a2a5aa486c1908c530bfda06dd (IExperimentManager)
9a41649aeea90fc3625f383aaea33e5efe2c37ea (Thiemo, PHPDoc)
582cf4260f0c43f588b0b9dc0a68b1ef3c0e6a97 (Urbanecm, cleanup)
d9bbbc9b28c4586551d33c09e8f1f111539d6de3 (Urbanecm, test)
```

(the last two patches also need to be pulled to wmf.17, the rest is already there)

Doing this now...

Urbanecm_WMF added a subscriber: **gerritbot**. 2026-02-25 16:03:42 (UTC+0)

Change #1243874 had a related patch set uploaded (by Urbanecm; author: Urbanecm): [mediawiki/extensions/GrowthExperiments@master] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 16:03:52 (UTC+0)

Change #1243874 **merged** by jenkins-bot: [mediawiki/extensions/GrowthExperiments@master] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 16:37:37 (UTC+0)

Jdforrester-WMF added a project: ~~**MW-1.46-notes (1.46.0-wmf.18; 2026-03-03)**~~. 2026-02-25 17:17:31 (UTC+0)

Change #1244011 had a related patch set uploaded (by Urbanecm; author: Urbanecm): [mediawiki/extensions/GrowthExperiments@wmf/1.46.0-wmf.17] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 23:09:28 (UTC+0)

Change #1244012 had a related patch set uploaded (by Urbanecm; author: Urbanecm): [mediawiki/extensions/GrowthExperiments@wmf/1.46.0-wmf.16] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 23:09:53 (UTC+0)

Change #1244012 **merged** by jenkins-bot: [mediawiki/extensions/GrowthExperiments@wmf/1.46.0-wmf.16] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 23:24:38 (UTC+0)

Change #1244011 **merged** by jenkins-bot: [mediawiki/extensions/GrowthExperiments@wmf/1.46.0-wmf.17] SECURITY: ReassignMentees: Handle hidden users correctly 2026-02-25 23:24:44 (UTC+0)

Urbanecm_WMF added a subscriber: **ReleaseTaggerBot**. 2026-02-25 23:33:17 (UTC+0)

Urbanecm changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2026-02-25 23:39:23 (UTC+0)

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

Urbanecm_WMF moved this task from **Doing** to **QA** on the ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~ board. 2026-02-25 23:41:50 (UTC+0)

Mission succeeded. The amount of `reassignMenteesJob` jobs should drop.

ReleaseTaggerBot edited projects, added ~~**MW-1.46-notes (1.46.0-wmf.17; 2026-02-24)**~~; removed ~~**MW-1.46-notes (1.46.0-wmf.18; 2026-03-03)**~~. 2026-02-26 00:00:13 (UTC+0)

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2026-03-02 17:26:59 (UTC+0)

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

sbassett added subscribers: **ASanford-WMF**, **sbassett**.

Thanks for the quick work to fix this issue and get it deployed and backported! **@ASanford-WMF** will track this for the next Wikimedia supplemental security release (**T411394**).

ASanford-WMF 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)**. 2026-03-03 19:46:46 (UTC+0)

DMburugu moved this task from **QA** to **Test in Production** on the ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~ board. 2026-03-10 14:48:43 (UTC+0)

DMburugu edited projects, added ~~**Growth-Team (FY2025-26 Q3 Sprint 5)**~~; removed ~~**Growth-Team (FY2025-26 Q3 Sprint 4)**~~. 2026-03-11 11:17:55 (UTC+0)

DMburugu moved this task from **Incoming** to **Test in Production** on the ~~**Growth-Team (FY2025-26 Q3 Sprint 5)**~~ board.

Etonkovidova closed this task as *Resolved*. 2026-03-13 18:22:40 (UTC+0)

Checked https://logstash.wikimedia.org/goto/9d01ba6b23f6f82853c3e50f1bc0cc17 for `ReassignMenteesJob` - the number of reports is low now.

sbassett added a comment. 2026-03-13 21:05:17 (UTC+0)

The security patches were pushed through gerrit I believe, so we should be fine to make this task public now, correct, **@Urbanecm_WMF** ?

Mstyles renamed this task from *With hidden mentees, ReassignMenteesJob runs as an infinite loop* to *CVE-2026-39934: With hidden mentees, ReassignMenteesJob runs as an infinite loop*. 2026-04-07 22:29:22 (UTC+0)

A_smart_kitten subscribed. 2026-04-08 10:15:22 (UTC+0)