CVE-2022-39194: Growth's Community configuration makes it possible for rogue admin to take down a site

Actions

Closed, Resolved Public SECURITY

Assigned To

Tgr

Authored By

Urbanecm_WMF
2022-07-18 09:26:59 (UTC+0)

Tags

Security-Team (Our Part Is Done)
Security
GrowthExperiments-CommunityConfiguration
Growth-Team (Current Sprint) (QA)
SecTeam-Processed (Completed)
Vuln-DoS (Tracked)
MW-1.39-notes (1.39.0-wmf.27; 2022-08-29)

Referenced Files

F35321380: 0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch
2022-07-19 09:02:07 (UTC+0)

F35321233: 0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch
2022-07-19 05:57:20 (UTC+0)

Subscribers

Aklapper
DMburugu
Etonkovidova
gerritbot
kostajh
RhinosF1
sbassett

View All 10 Subscribers

Description

Steps to reproduce

1. All the steps below need to be done from an account with sysop access
2. Ensure MediaWiki:GrowthExperimentsConfig.json does not exist. If it exists, move it to a different title or delete it.
3. Create MediaWiki:Foo.json with **P31294** as the content (this content does not meet constraints set by `GrowthConfigValidation`; `GEHelpPanelViewMoreTitle` is int, should be string)
4. Move MediaWiki:Foo.json to MediaWiki:GrowthExperimentsConfig.json
5. Wait for a day, or run `\MediaWiki\MediaWikiServices::getInstance()->get('GrowthExperimentsWikiPageConfigLoader')->invalidate(Title::newFromText('MediaWiki:GrowthExperimentsConfig.json'))` in eval.php / shell.php session

Expected behavior

Wiki is up. No config from MediaWIki:GrowthExperimentsConfig.json is used (site should fall back to whatever the globals say). Logs (GrowthExperiments channel) complain about the fallback happening.

Observed behavior

Wiki is fully down (**P31296** is the traceback).

Details

Risk Rating
High

Author Affiliation
WMF Product

	Project	Subject
	mediawiki/extensions/GrowthExperiments	SECURITY: Don't use messages in WikiPageConfig error handler
	mediawiki/extensions/GrowthExperiments	SECURITY: Don't use messages in WikiPageConfig error handler
	mediawiki/extensions/GrowthExperiments	SECURITY: Don't use messages in WikiPageConfig error handler

Customize query in gerrit

Related Objects

Mentions

Mentioned In
~~T311785: Write and send supplementary release announcement for extensions and skins with security patches (1.35.8/1.37.5/1.38.3)~~

Mentioned Here
rEGREc8fb5fadeda0: Move MessageCache::get hook to a separate hook handler
~~T311785: Write and send supplementary release announcement for extensions and skins with security patches (1.35.8/1.37.5/1.38.3)~~
~~T313254: There should be a way to reliably validate a JSON content + title combination~~
P31294 Dangerous version of MediaWiki:GrowthExperimentsConfig.json
P31296 (An Untitled Masterwork)

Urbanecm_WMF created this task. 2022-07-18 09:26:59 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2022-07-18 09:27:01 (UTC+0)

Urbanecm_WMF added a project: **GrowthExperiments-CommunityConfiguration**. 2022-07-18 09:27:15 (UTC+0)

Restricted Application added a project: **Growth-Team**. · View Herald Transcript 2022-07-18 09:27:17 (UTC+0)

Urbanecm_WMF added a comment. 2022-07-18 12:13:47 (UTC+0)

Roughly, this is what happens:

1. A message is requested by our own code, core, or another extension
2. `HomepageHooks` is constructed, `GrowthExperimentsCampaignConfig` is constructed as one of `HomepageHooks` ' dependencies
3. `GrowthExperimentsCampaignConfig` 's service wiring needs `GECampaigns` , which is stored within community configuration
4. `WikiPageConfig::getConfigData` calls `WikiPageConfigLoader` , which returns an invalid configuration
5. `WikiPageConfig::getConfigData` attempts to log into the error log, and to construct a reason for the error by calling `Status::wrap( $res )->getWikiText( false, false, 'en' )`
6. `Status` attempts to request a couple of additional messages
7. Back to step 1, circular dependency happened.

The easiest fix would be to not call `Status::wrap( $res )->getWikiText( false, false, 'en' )` (and log message keys + parameters only instead). Alternatively, we can move `HomepageHooks::onMessageCache__get` to a new hook.

kostajh triaged this task as *High* priority. 2022-07-18 17:25:11 (UTC+0)

kostajh edited projects, added **Growth-Team (Current Sprint)**; removed **Growth-Team**.

> *The easiest fix would be to not call Status::wrap($res)->getWikiText(false, false, 'en') (and log message keys + parameters only instead).*

I think let's go with that option.

Tgr added a comment. 2022-07-18 17:55:04 (UTC+0)

Basically this error has two components, right?

1. Someone sets up an invalid Growth config page in some manner that circumvents our edit hook (which would prevent saving an invalid config page).
2. There is a circular dependency in the error handling logic for an invalid Growth config page.

I don't think #1 has a good fix, nor that it really needs to be fixed. We could add a check to the MovePageIsValidMove hook, but there are so many nonconventional ways for a sufficiently privileged user to create a page (import, undelete, revert...), it's a lot of effort to check all of those, not a good time investment IMO.

> In ~~**T313205#8084201**~~, **@Urbanecm_WMF** wrote:
>
> *The easiest fix would be to not call* `Status::wrap( $res )->getWikiText( false, false, 'en' )` *(and log message keys + parameters only instead).*

IMO we should do that - it's always a good idea to avoid message rendering in error handling logic, MediaWiki's message rendering is incredibly complex (involves DB access, page access, multiple cache layers, invoking the parser...). The scenario described in this task is pretty unlikely, but if we accidentally roll out a change to configuration validation which is not backwards compatible, it would be nice for that to not break the wikis immediately.

> *Alternatively, we can move* `HomepageHooks::onMessageCache__get` *to a new hook.*

IMO we should do that as well. MessageCache hooks are scary, MediaWiki uses messages all around the place, often invisibly, including e.g. some exception handling and relatively early setup. It would be much preferable not to interfere with it. I think we can just use a skin hook instead?

Tgr added a comment. 2022-07-18 18:13:46 (UTC+0)

Security-Team can we use Gerrit for the fixes? I don't think there is any risk of this being exploited as you'd need admin permissions + it seems hard to reverse-engineer this vulnerability from the fixes.

Tgr added a comment. 2022-07-18 18:29:35 (UTC+0)

Filed ~~**T313254: There should be a way to reliably validate a JSON content + title combination**~~ about what's IMO the underlying architectural problem for step #1.

sbassett added subscribers: **gerritbot**, **sbassett**. 2022-07-18 20:27:09 (UTC+0)

> In ~~**T313205#8085582**~~, **@Tgr** wrote:

> *Security-Team* *can we use Gerrit for the fixes? I don't think there is any risk of this being exploited as you'd need admin permissions + it seems hard to reverse-engineer this vulnerability from the fixes.*

IIUC, the exploit requires:

1. a rogue or compromised admin on a project where ext:GrowthExperiments is enabled
2. a 24-hour config cache invalidation period after setting the bad config (or deployment rights)

I think the risk is probably ⚠ **high** in that this can bring down an *entire wiki*, but the knowledge and rights that are required to perform the exploit are also fairly high. If the patches are going to be fairly complex, then gerrit is fine given the assumptions above. Ideally, somewhat-vague commit messages/comments would be employed and this could be merged before the train cut, but I know we're pretty close to that happening for this week.

sbassett moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2022-07-18 20:27:35 (UTC+0)

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

sbassett added a project: **Vuln-DoS**.

sbassett changed Risk Rating from N/A to High.

Urbanecm_WMF added a comment. 2022-07-18 21:11:01 (UTC+0)

> In ~~**T313205#8085509**~~, **@Tgr** wrote:
>
> *Basically this error has two components, right?*
>
> 1. *Someone sets up an invalid Growth config page in some manner that circumvents our edit hook (which would prevent saving an invalid config page).*
> 2. *There is a circular dependency in the error handling logic for an invalid Growth config page.*
>
> *I don't think #1 has a good fix, nor that it really needs to be fixed. We could add a check to the MovePageIsValidMove hook, but there are so many nonconventional ways for a sufficiently privileged user to create a page (import, undelete, revert...), it's a lot of effort to check all of those, not a good time investment IMO.*

Agreed.

> > *Alternatively, we can move* `HomepageHooks::onMessageCache__get` *to a new hook.*
>
> *IMO we should do that as well. MessageCache hooks are scary, MediaWiki uses messages all around the place, often invisibly, including e.g. some exception handling and relatively early setup. It would be much preferable not to interfere with it. I think we can just use a skin hook instead?*

FTR, I originally meant to say "to a new hook *handler*" (that should remove the GrowthExperimentsCampaignConfig dependency, and break the circle). However, using a different hook for the reasons you described makes also sense.

Tgr added a comment. 2022-07-19 05:57:20 (UTC+0)

> In ~~T313205#8086073~~, **@sbassett** wrote:
>
> *a 24-hour config cache invalidation period after setting the bad config (or deployment rights)*

Although that can probably be circumvented by editing another configuration file, which triggers invalidation. So maybe better to do a proper security patch. Attached:

0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch 1 KB
Download

The other patch is going to be complicated so I'd rather do it in Gerrit, but either patch is enough to prevent the issue.

Tgr claimed this task. 2022-07-19 06:23:57 (UTC+0)

Tgr moved this task from **Incoming** to **Code Review** on the **Growth-Team (Current Sprint)** board.

kostajh added a comment. 2022-07-19 08:17:44 (UTC+0)

> In ~~T313205#8086660~~, **@Tgr** wrote:
>
> > In ~~T313205#8086073~~, **@sbassett** wrote:
> >
> > *a 24-hour config cache invalidation period after setting the bad config (or deployment rights)*
>
> *Although that can probably be circumvented by editing another configuration file, which triggers invalidation. So maybe better to do a proper security patch. Attached:*
>
> ***0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch*** *1 KB*
> *Download*
>
> *The other patch is going to be complicated so I'd rather do it in Gerrit, but either patch is enough to prevent the issue.*

Virtual +2 from me.

Urbanecm_WMF added a comment. 2022-07-19 09:02:07 (UTC+0)

0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch 1 KB
Download

Slightly amended the commit message (the standard prefix is `SECURITY:` ; `[SECURITY]` gets lost during applying the patch file) and deployed:

```
11:00 <urbanecm> !log Deployed patch for T313205
11:00 <+stashbot> Logged the message at https://wikitech.wikimedia.org/wiki/Server_Admin_Log
```

kostajh added a comment. 2022-07-20 05:24:36 (UTC+0)

> In ~~T313205#8086932~~, **@Urbanecm_WMF** wrote:
>
> ***0001-SECURITY-Don-t-use-messages-in-WikiPageConfig-error-.patch*** *1 KB*
> *Download*
>
> *Slightly amended the commit message (the standard prefix is `SECURITY:`; `[SECURITY]` gets lost during applying the patch file) and deployed:*
>
> ```
> 11:00 <urbanecm> !log Deployed patch for T313205
> 11:00 <+stashbot> Logged the message at https://wikitech.wikimedia.org/wiki/Server_Admin_Log
> ```

Thanks **@Urbanecm_WMF**. We can lift the security tag now? After that, we need a gerrit patch as well, right?

Tgr added a comment. 2022-07-20 08:40:45 (UTC+0)

> In ~~T313205#8085509~~, **@Tgr** wrote:
>
> > In ~~T313205#8084201~~, **@Urbanecm_WMF** wrote:
> >
> > *Alternatively, we can move `HomepageHooks::onMessageCache__get` to a new hook.*
>
> *IMO we should do that as well. MessageCache hooks are scary, MediaWiki uses messages all around the place, often invisibly, including e.g. some exception handling and relatively early setup. It would be much preferable not to interfere with it. I think we can just use a skin hook instead?*

I'm giving up on that - it seems almost but not quite possible, and I already spent more time on it than it was worth. (c815678 was my attempt - it mostly works, except in new Vector for some reason.

> In ~~T313205#8086158~~, **@Urbanecm_WMF** wrote:
>
> *FTR, I originally meant to say "to a new hook* handler" *(that should remove the GrowthExperimentsCampaignConfig dependency, and break the circle).*

I did that eventually. The patch is https://gerrit.wikimedia.org/r/c/mediawiki/extensions/GrowthExperiments/+/815687 .

Urbanecm_WMF added a comment. 2022-07-20 20:12:28 (UTC+0)

> In ~~T313205#8089972~~, **@kostajh** wrote:
>
> *Thanks **@Urbanecm_WMF**. We can lift the security tag now? After that, we need a gerrit patch as well, right?*

IMO, yes, but I usually defer to **@sbassett** / Security-Team to decide when to publish a task.

sbassett added a comment. 2022-07-20 22:15:55 (UTC+0)

Thanks for the patch and deploy, **@Tgr** and **@Urbanecm_WMF**! We can track this for the next supplemental security release (~~**T311785**~~).

> *IMO, yes, but I usually defer to* ***@sbassett*** */* *Security-Team* *to decide when to publish a task.*

I don't see anything on the bug that looks particularly sensitive, especially since we're patched in prod. If you're ready to make this public to start on the backports, etc. feel free to do so. Or I can make it public if you'd prefer.

sbassett mentioned this in ~~**T311785: Write and send supplementary release announcement for extensions and skins with security patches (1.35.8/1.37.5/1.38.3)**~~. 2022-07-20 22:16:34 (UTC+0)

Tgr added a comment. 2022-08-17 01:54:43 (UTC+0)

FWIW this should now be fixed in production even without the security patch, due to **rEGREc8fb5fadeda0: Move MessageCache::get hook to a separate hook handler**. Let's do it.

sbassett changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2022-08-17 01:58:02 (UTC+0)

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

Tgr added a comment. 2022-08-17 01:59:14 (UTC+0)

...although on reflection I have no idea how to do it. In the past when security tasks used the same task type, I could edit access settings, but I think now it would require a task type change? And I either don't have permission for that, or just can't figure where it's located on the UI.

sbassett added a comment. 2022-08-17 02:12:50 (UTC+0)

@Tgr - I just made it public (both the edit and view policy). Also added a note about the currently-deployed security patch here: T276237#8160184.

RhinosF1 added a subscriber: **RhinosF1**. Edited · 2022-08-17 07:40:45 (UTC+0)

P31294 and **P31296** are linked to this task. Any reason for them to remain private?

Urbanecm_WMF added a comment. 2022-08-17 09:06:15 (UTC+0)

> In ~~**T313205#8160456**~~, **@RhinosF1** wrote:
> ***P31294*** *and* ***P31296*** *are linked to this task. Any reason for them to remain private?*

I don't think so -- I created them privately only because the task was private. Both pastes should be now public.

RhinosF1 added a comment. 2022-08-17 09:07:15 (UTC+0)

Thanks!

gerritbot added a comment. 2022-08-23 04:16:59 (UTC+0)

Change 825454 had a related patch set uploaded (by Gergő Tisza; author: Gergő Tisza):

[mediawiki/extensions/GrowthExperiments@master] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825454

gerritbot added a project: **Patch-For-Review**. 2022-08-23 04:16:59 (UTC+0)

gerritbot added a comment. 2022-08-23 04:20:41 (UTC+0)

Change 825282 had a related patch set uploaded (by Gergő Tisza; author: Gergő Tisza):

[mediawiki/extensions/GrowthExperiments@REL1_38] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825282

gerritbot added a comment. 2022-08-23 04:21:26 (UTC+0)

Change 825283 had a related patch set uploaded (by Gergő Tisza; author: Gergő Tisza):

[mediawiki/extensions/GrowthExperiments@REL1_37] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825283

Tgr added a comment. 2022-08-23 04:31:49 (UTC+0)

Uploaded & backported to 1.37 and 1.38; the relevant code did not exist yet in 1.35.

gerritbot added a comment. 2022-08-23 09:47:57 (UTC+0)

Change 825454 **merged** by jenkins-bot:

[mediawiki/extensions/GrowthExperiments@master] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825454

ReleaseTaggerBot added a project: ~~**MW-1.39-notes (1.39.0-wmf.27; 2022-08-29)**~~. 2022-08-23 10:00:58 (UTC+0)

gerritbot added a comment. 2022-08-24 05:05:18 (UTC+0)

Change 825282 **merged** by Gergő Tisza:

[mediawiki/extensions/GrowthExperiments@REL1_38] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825282

gerritbot added a comment. 2022-08-24 05:29:13 (UTC+0)

Change 825283 **merged** by jenkins-bot:

[mediawiki/extensions/GrowthExperiments@REL1_37] SECURITY: Don't use messages in WikiPageConfig error handler

https://gerrit.wikimedia.org/r/825283

Maintenance_bot removed a project: **Patch-For-Review**. 2022-08-24 05:30:24 (UTC+0)

Tgr moved this task from **Code Review** to **QA** on the **Growth-Team (Current Sprint)** board.
2022-08-24 09:27:59 (UTC+0)

This is done from our perspective. **@sbassett** do you prefer leaving it open until the next release, or track that elsewhere?

sbassett lowered the priority of this task from *High* to *Low*. 2022-08-24 15:16:44 (UTC+0)

> In ~~**T313205#8180759**~~, **@Tgr** wrote:
> *This is done from our perspective.* ***@sbassett*** *do you prefer leaving it open until the next release, or track that elsewhere?*

Sure, it's tracked for the next supplemental release at ~~**T311785**~~. We can leave this task open or in-progress until that release happens towards the end of the quarter, where this (now-public) issue will be re-announced. And I think we can bump down the priority now as well.

RhinosF1 renamed this task from *Growth's Community configuration makes it possible for rogue admin to take down a site* to *CVE-2022-39194: Growth's Community configuration makes it possible for rogue admin to take down a site*.
2022-09-02 06:40:59 (UTC+0)

Etonkovidova closed this task as *Resolved*. 2022-09-07 22:20:17 (UTC+0)

sbassett moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board.
2022-10-06 16:33:49 (UTC+0)