Maniphest T418254 Create Task

CVE-2026-39934: Stored XSS through system messages on the contributions tab of Special:EventDetails

Actions

Closed, Resolved Public SECURITY

Assigned To

Daimona

Authored By

Daimona
2026-02-24 15:21:25 (UTC+0)

Tags

Security-Team (Watching)

Security

Connection-Team (Connection-Current-Sprint) (QA 🐛)

CampaignEvents (Backlog)

Vuln-XSS

Patch-For-Review

SecTeam-Processed (Completed)

MW-1.46-notes (1.46.0-wmf.20; 2026-03-17)

Referenced Files

F72316863: T418254.patch
2026-02-24 15:30:00 (UTC+0)

Subscribers

Aklapper

cmelo

Daimona

gerritbot

ifried

JFernandez-WMF

ldelench_wmf

View All 12 Subscribers

Description

The localised wiki names displayed on the "Contributions" tab of Special:EventDetails are coming from the `project-localized-name-*` messages, and are output without escaping (`text()` only).

Details

Risk Rating
Low

Author Affiliation
WMF Product

RELATED CHANGES IN GERRIT:

	Subject	Repo
	SECURITY: EventContributionsPager: escape wiki names for display	mediawiki/extensions/CampaignEvents

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)

Mentioned Here
~~T413811: 1.46.0-wmf.20 deployment blockers~~
~~T410374: Show user-friendly wiki names in the contributions table~~

Daimona created this task. 2026-02-24 15:21:25 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2026-02-24 15:21:27 (UTC+0)

Daimona claimed this task. 2026-02-24 15:22:54 (UTC+0)

Daimona added projects: **Connection-Team (Connection-Current-Sprint)**, **CampaignEvents**, **Vuln-XSS**.

Daimona moved this task from **Upcoming / refining** 💡 to **Code Review** 💬 on the **Connection-Team (Connection-Current-Sprint)** board. 2026-02-24 15:29:59 (UTC+0)

Daimona added a project: **Patch-For-Review**.

Proposed patch:

T418254.patch 1 KB
Download

This code was introduced in r1206829 (for ~~T410374~~), on 2025-11-27. This is not part of any MW release, so it only needs to be fixed in master (no backports needed).

Daimona added subscribers: **JFernandez-WMF**, **ldelench_wmf**, **ifried** and **3 others**. 2026-02-24 15:31:32 (UTC+0)

sbassett subscribed. 2026-02-24 19:25:24 (UTC+0)

> In ~~T418254#11645995~~, **@Daimona** wrote:
>
> *Proposed patch:*
>
> ***T418254.patch*** *1 KB*
> *Download*

CR+2, LGTM. I think we can try to get this deployed during next Monday's (2026-03-02) security window.

sbassett changed the task status from *Open* to *In Progress*. 2026-03-02 17:19:18 (UTC+0)

sbassett triaged this task as *Medium* priority.

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board.

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

Daimona added a comment. 2026-03-05 14:01:41 (UTC+0)

@sbassett Hi, has the patch been deployed? If so, can we proceed with the public patch now, considering that it only needs a master fix per ~~T418254#11645995~~.

sbassett added a comment. 2026-03-05 14:56:00 (UTC+0)

> In ~~T418254#11677562~~, **@Daimona** wrote:
>
> ***@sbassett*** *Hi, has the patch been deployed? If so, can we proceed with the public patch now, considering that it only needs a master fix per* ~~***T418254#11645995***~~*.*

Hey, sadly, it looks like this one didn't go out during Monday's window. I can try to get it out today after the late backport window. And then we can open up the task.

Mstyles moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board.
2026-03-05 22:46:55 (UTC+0)

Mstyles subscribed.

> In ~~T418254#11645995~~, **@Daimona** wrote:

> *Proposed patch:*
>
> **T418254.patch** 1 KB
> Download
>
> *This code was introduced in r1206829 (for **T410374**), on 2025-11-27. This is not part of any MW release, so it only needs to be fixed in master (no backports needed).*

Deployed

Mstyles 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)**. 2026-03-05 22:50:29 (UTC+0)

Daimona added a comment. 2026-03-06 23:59:55 (UTC+0)

> In ~~T418254#11679671~~, @**Mstyles** wrote:
>
> *Deployed*

Thanks! Can I proceed with the public fix now then?

sbassett added a subscriber: **gerritbot**. 2026-03-08 16:21:24 (UTC+0)

> In ~~T418254#11684076~~, @**Daimona** wrote:
>
> > In ~~T418254#11679671~~, @**Mstyles** wrote:
> >
> > *Deployed*
>
> *Thanks! Can I proceed with the public fix now then?*

Yes.

Change #1249320 had a related patch set uploaded (by Daimona Eaytoy; author: Daimona Eaytoy): 2026-03-09 14:23:31 (UTC+0)
[mediawiki/extensions/CampaignEvents@master] SECURITY: EventContributionsPager: escape wiki names for display

Change #1249320 **merged** by jenkins-bot: 2026-03-13 11:47:17 (UTC+0)
[mediawiki/extensions/CampaignEvents@master] SECURITY: EventContributionsPager: escape wiki names for display

Daimona moved this task from **Code Review** 💬 to **QA** 🐛 on the **Connection-Team (Connection-Current-Sprint)** board. 2026-03-13 14:08:39 (UTC+0)

The fix can be verified with $wgUseXssLanguage on a non-empty contribution tab.

And it should be possible to undeploy the security patch with next week's train.

Jdforrester-WMF added a project: ~~**MW-1.46-notes (1.46.0-wmf.20; 2026-03-17)**~~. 2026-03-13 14:23:25 (UTC+0)

sbassett changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2026-03-13 16:02:59 (UTC+0)

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

sbassett changed Risk Rating from N/A to Low.

SecurityPatchBot changed the task status from *In Progress* to *Open*. 2026-03-14 00:53:37 (UTC+0)

SecurityPatchBot raised the priority of this task from *Medium* to *Unbreak Now!*.

SecurityPatchBot added a parent task: ~~**T413811: 1.46.0-wmf.20 deployment blockers**~~.

Patch is blocking upcoming release

Patch `01-T418254.patch` is currently failing to apply for the most recent code in the mainline branch of `extensions/CampaignEvents`. This is blocking MediaWiki release `1.46.0-wmf.20` (~~**T413811**~~)

If the patch needs to be rebased

A new version of the patch can be placed at the right location in the deployment server with the following Scap command:

```
REVISED_PATCH=<path_to_revised_patch>
scap update-patch --message-body 'Rebase to solve merge conflicts'
/srv/patches/next/extensions/CampaignEvents/01-T418254.patch "$REVISED_PATCH"
```

If the patch has been made public

The patch can be dropped in the deployment server with the following Scap command:

```
scap remove-patch --message-body 'Dropping patch already made public'
/srv/patches/next/extensions/CampaignEvents/01-T418254.patch
```

Zabe changed the task status from *Open* to *In Progress*. 2026-03-14 00:56:55 (UTC+0)

Zabe lowered the priority of this task from *Unbreak Now!* to *Medium*.

Zabe subscribed.

```
commit a7829842fd2c224b75d24428ad0cab8631d73b82 (HEAD -> master)
Author: Alexander Vorwerk <zabe@avorwerk.net>
Date:   Sat Mar 14 00:55:51 2026 +0000

    Scap remove-patch: removed 1 patch
```

```
    Dropping patch already made public

    Removed patches:
    next:
      - extensions/CampaignEvents/01-T418254.patch
```

Zabe removed a parent task: ~~**T413811: 1.46.0-wmf.20 deployment blockers**~~. 2026-03-14 00:57:18 (UTC+0)

MHorsey-WMF added a comment. 2026-03-16 11:21:36 (UTC+0)

@Daimona as this patch failed to deploy, does it require more work?

MHorsey-WMF moved this task from **QA** 🐛 to **Ready for development** on the **Connection-Team (Connection-Current-Sprint)** board. 2026-03-16 11:22:15 (UTC+0)

Daimona moved this task from **Ready for development** to **QA** 🐛 on the **Connection-Team (Connection-Current-Sprint)** board. 2026-03-16 14:24:22 (UTC+0)

> In ~~**T418254#11713035**~~, **@MHorsey-WMF** wrote:
>
> *@Daimona as this patch failed to deploy, does it require more work?*

No, the patch has landed in master and testing instructions from ~~**T418254#11706736**~~ are still valid.

The bot in ~~**T418254#11709279**~~ warned that the previously applied private patch in production would no longer apply with this week's train due to a conflict, which is expected because the fix is now public. BUT, the fix was not backported to wmf.19; so, does that mean that production is currently not patched?

sbassett added a comment. 2026-03-16 15:32:00 (UTC+0)

> In ~~**T418254#11713904**~~, **@Daimona** wrote:
>
> *The bot in ~~**T418254#11709279**~~ warned that the previously applied private patch in production would no longer apply with this week's train due to a conflict, which is expected because the fix is now public. BUT, the fix was not backported to wmf.19; so, does that mean that production is currently not patched?*

The patch is still on wmf.19 in production:

```
( ^◡^)> pwd
/srv/mediawiki-staging/php-1.46.0-wmf.19/extensions/CampaignEvents
```

```
( ^◡^)> git log --graph --decorate --oneline -n5
* b363c975 (HEAD) SECURITY: EventContributionsPager: escape wiki names for display
...
```

Since the master patch got merged last week, it should make the cut today for wmf.20. And then the wmf.19 patch will "fall off" production. SecurityPatchBot is just aggressive in trying to call out potential conflicts with security patches before they happen.

Daimona added a comment. 2026-03-16 15:33:30 (UTC+0)

I see, thank you! I'm not familiar with the process, hence my question. I'll keep that in mind going forwards.

sbassett added a comment. Edited · 2026-03-16 15:42:08 (UTC+0)

> In ~~T418254#11714197~~, @**Daimona** wrote:
> *I see, thank you! I'm not familiar with the process, hence my question. I'll keep that in mind going forwards.*

Sure, the high-level process looks a bit like:

1. We push security patches up to deployment under various version-related staging directories
2. We deploy these patches via scap, typically during the Monday security deployment window, but sometimes throughout the week
3. If any of those patches conflict (due to public changes in the code or publicly merging the security patch), SecurityPatchBot uses a "next" directory to try to find these issues early and alert the security team and release engineering
4. The aforementioned process ^ doesn't directly remove or modify any existing, applied security patches within Wikimedia production, it just alerts
5. Though scap won't apply any conflicting security patches (technically it can't anyways) it finds (it considers them "dropped" or "released" in this context)
6. The dropped/released security patches get cleaned up by the security team or release engineering throughout the week

Daimona added a comment. 2026-03-16 17:24:18 (UTC+0)

Thanks for the explanation, bookmarked for future reference :D

So, this task can be QAed as noted in **T418254#11706736**.

Mstyles renamed this task from *XSS-via-i18n in localised wiki names on the contributions tab of Special:EventDetails* to *CVE-2026-39934: XSS-via-i18n in localised wiki names on the contributions tab of Special:EventDetails*. 2026-04-07 22:30:15 (UTC+0)

Mstyles closed this task as *Resolved*.

sbassett renamed this task from *CVE-2026-39934: XSS-via-i18n in localised wiki names on the contributions tab of Special:EventDetails* to *CVE-2026-39934: Stored XSS through system messages on the contributions tab of Special:EventDetails*. 2026-04-08 15:08:27 (UTC+0)