Maniphest T418179 Create Task

CVE-2026-39933: Multiple XSS vulnerabilities in GlobalWatchlist

Actions

Closed, Resolved Public SECURITY

Assigned To

SomeRandomDeveloper

Authored By

SomeRandomDeveloper
2026-02-23 22:13:53 (UTC+0)

Tags

Security-Team (Watching)

Security

MediaWiki-extensions-GlobalWatchlist (In progress)

Vuln-XSS

affects-Miraheze (Backlog)

SecTeam-Processed (Completed)

Referenced Files

F72296008: T418179.patch
2026-02-23 22:25:16 (UTC+0)

F72295957: Pasted image 20260223224206.png
2026-02-23 22:13:53 (UTC+0)

F72295955: Pasted image 20260223223702.png
2026-02-23 22:13:53 (UTC+0)

F72295949: Pasted image 20260223222623.png
2026-02-23 22:13:53 (UTC+0)

F72295943: Pasted image 20260223221149.png
2026-02-23 22:13:53 (UTC+0)

F72295939: Pasted image 20260223220053.png
2026-02-23 22:13:53 (UTC+0)

Subscribers

Aklapper

gerritbot

IKhitron

Mstyles

sbassett

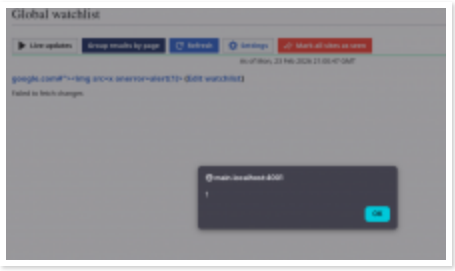
SomeRandomDeveloper

Description

The GlobalWatchlist extension is vulnerable to self-XSS (when used without CentralAuth) and stored XSS through system messages.

Self-XSS through Settings

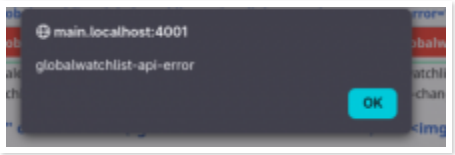
1. Make sure CentralAuth is disabled
2. Go to `Special:GlobalWatchlistSettings` and add a new site with the following URL to the user defined site list: `google.com#"><img src=x onerror=alert(1)>`
3. Go to `Special:GlobalWatchlist`



Cause: https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/Linker.js#L27-L30 and https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/SiteBase.js#L101 The site list is not validated if CentralAuth is disabled or if GlobalWatchlist failed to retrieve a list of valid wikis for any other reason.

i18n XSS through 'globalwatchlist-api-error'

1. Add `$wgUseXssLanguage = true;` to your LocalSettings.php
2. Go to `Special:GlobalWatchlist?uselang=x-xss`
3. Cause an API query made by the extension to fail for any reason (locally it does this for example if CORS is not configured properly, the other wiki is offline, etc)



Cause: https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/SiteBase.js#L101

Insufficient escaping in user links

Usernames in user links are not escaped sufficiently, which allows breaking out of attributes, e.g. with the username `"test username`:

The unescaped username is also inserted into the HTML contents of the link.
However, `$wgInvalidUsernameCharacters` contains `=` since 1.40, and `>` cannot be used either, so it's likely not possible to perform XSS here.
Cause: https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/WatchlistUtils.js#L142-L145

i18n XSS through 'parentheses'

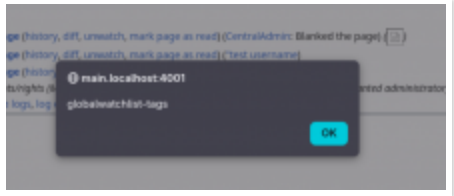
1. Add `$wgUseXssLanguage = true;` to your LocalSettings.php
2. Make sure there are edits with tags on your global watchlist
3. Go to `Special:GlobalWatchlist?uselang=x-xss`
4. Click on "Group results by page" (this was necessary for me so an edit with a tag would show up)

Cause: https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/WatchlistUtils.js#L402

i18n XSS through 'globalwatchlist-tags'

This is not detectable through `?uselang=x-xss` because the message is wrapped in the `parentheses` message.

1. Edit `MediaWiki:Globalwatchlist-tags` to `<img src=x onerror=alert('globalwatchlist-tags')>`
2. Go to `Special:GlobalWatchlist`
3. Click on "Group results by page" (this was necessary for me so an edit with a tag would show up)



Cause: https://github.com/wikimedia/mediawiki-extensions-GlobalWatchlist/blob/24816af182281a6da8a17a6521cfba1b4458a9f3/modules/specialglobalwatchlist/WatchlistUtils.js#L401

Additional information

MW: **e606cf78f98ea4d365edb28ffc93eb26719c2d57** (1.46.0-alpha)
GlobalWatchlist: **24816af182281a6da8a17a6521cfba1b4458a9f3**

Details

Author Affiliation
Wikimedia Communities

RELATED CHANGES IN GERRIT:

	Subject	Repo
	SECURITY: Fix multiple XSS vulnerabilities	mediawiki/extensions/GlobalWatchlist
	SECURITY: Fix multiple XSS vulnerabilities	mediawiki/extensions/GlobalWatchlist
	SECURITY: Fix multiple XSS vulnerabilities	mediawiki/extensions/GlobalWatchlist
	SECURITY: Fix multiple XSS vulnerabilities	mediawiki/extensions/GlobalWatchlist

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

Status	Assigned	Task
		Restricted Task
Resolved	SomeRandomDeveloper	~~T418179~~ CVE-2026-39933: Multiple XSS vulnerabilities in GlobalWatc…

SomeRandomDeveloper created this task. 2026-02-23 22:13:53 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2026-02-23 22:13:55 (UTC+0)

SomeRandomDeveloper claimed this task. 2026-02-23 22:14:17 (UTC+0)

SomeRandomDeveloper added projects: **MediaWiki-extensions-GlobalWatchlist**, **Vuln-XSS**, **affects-Miraheze**.

SomeRandomDeveloper added a parent task: Restricted Task.

SomeRandomDeveloper added a project: **Patch-For-Review**. 2026-02-23 22:25:16 (UTC+0)

T418179.patch 4 KB
Download

SomeRandomDeveloper 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)**. 2026-02-23 23:13:22 (UTC+0)

sbassett changed the task status from *Open* to *In Progress*. 2026-03-02 17:22:22 (UTC+0)

sbassett triaged this task as *Medium* priority.

sbassett moved this task from **Backlog** to **In progress** on the **MediaWiki-extensions-GlobalWatchlist** board.

sbassett added subscribers: **Mstyles**, **sbassett**.

@Mstyles to review.

sbassett moved this task from **Incoming** to **In Progress** on the **Security-Team** board. 2026-03-02 17:22:43 (UTC+0)

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

Mstyles moved this task from **In Progress** to **Watching** on the **Security-Team** board. 2026-03-02 22:29:45 (UTC+0)

> In ~~**T418179#11642784**~~, **@SomeRandomDeveloper** wrote:
>
> ***T418179.patch*** *4 KB*
> *Download*

Deployed

SomeRandomDeveloper removed a project: **Patch-For-Review**. 2026-03-06 21:25:17 (UTC+0)

SomeRandomDeveloper added a subscriber: **gerritbot**. 2026-03-14 14:28:50 (UTC+0)

Change #1251948 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): 2026-03-14 14:30:51 (UTC+0)
[mediawiki/extensions/GlobalWatchlist@master] SECURITY: Fix multiple XSS vulnerabilities

Change #1251948 **merged** by jenkins-bot: 2026-03-14 14:46:00 (UTC+0)
[mediawiki/extensions/GlobalWatchlist@master] SECURITY: Fix multiple XSS vulnerabilities

Change #1251956 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/GlobalWatchlist@REL1_45] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 14:50:58 (UTC+0)

Change #1251964 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/GlobalWatchlist@REL1_44] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 15:09:20 (UTC+0)

Change #1251965 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/GlobalWatchlist@REL1_43] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 15:09:39 (UTC+0)

Change #1251964 **merged** by jenkins-bot: [mediawiki/extensions/GlobalWatchlist@REL1_44] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 15:29:27 (UTC+0)

Change #1251956 **merged** by jenkins-bot: [mediawiki/extensions/GlobalWatchlist@REL1_45] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 15:29:55 (UTC+0)

Change #1251965 **merged** by jenkins-bot: [mediawiki/extensions/GlobalWatchlist@REL1_43] SECURITY: Fix multiple XSS vulnerabilities — 2026-03-14 15:39:07 (UTC+0)

SomeRandomDeveloper closed this task as *Resolved*. 2026-03-14 22:33:00 (UTC+0)

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

SomeRandomDeveloper added a subscriber: **IKhitron**. 2026-03-16 12:43:22 (UTC+0)

IKhitron added a comment. 2026-03-16 12:48:29 (UTC+0)

Thank you for paying attention and for the fix, **@SomeRandomDeveloper**. And thank you for your answer in Gerrit as well.

Mstyles renamed this task from *Multiple XSS vulnerabilities in GlobalWatchlist* to *CVE-2026-39933: Multiple XSS vulnerabilities in GlobalWatchlist*. 2026-04-07 22:28:54 (UTC+0)

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

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