Maniphest T416502 Create Task

CVE-2026-22711: Stored XSS through system messages in WikiLove

Actions

Closed, Resolved Public SECURITY

Assigned To

SomeRandomDeveloper

Authored By

SomeRandomDeveloper
2026-02-04 17:45:40 (UTC+0)

Tags

Security-Team (Our Part Is Done)

Security

WikiLove (Backlog)

Vuln-XSS

affects-Miraheze (Backlog)

SecTeam-Processed (Completed)

Referenced Files

F71674401: T416502.patch
2026-02-04 17:51:17 (UTC+0)

F71674366: Pasted image 20260129194109.png
2026-02-04 17:45:40 (UTC+0)

Subscribers

Aklapper

gerritbot

Mstyles

sbassett

Scott_French

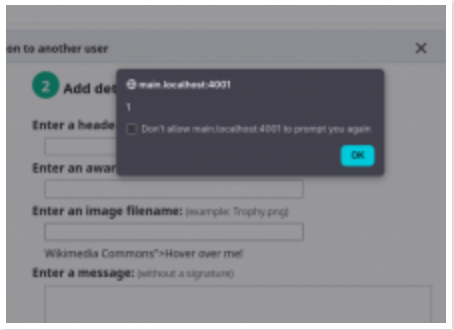
SomeRandomDeveloper

Description

Multiple system messages in WikiLove can be abused by users with the `editinterface` permission to execute arbitrary JS.

wikilove-commons-text/wikilove-commons-url

1. Edit `MediaWiki:Wikilove-commons-text` to `<div class="$1">Hover over me!</div>`
2. Edit `MediaWiki:Wikilove-commons-url` to `/onmouseenter=alert(1)//`
3. Make sure you have WikiLove enabled in your preferences
4. Go to a user page
5. Click on the heart icon next to the "View history" link
6. Click on "Make your own"
7. Hover over the text that says "Hover over me!"



wikilove-terms/wikilove-terms-url

The same steps as above can be done with `wikilove-terms` and `wikilove-terms-url`. The element is shown after previewing an award.

It's also possible to use a `javascript:` link in either `wikilove-commons-url` or `wikilove-terms-url`.

Cause

https://gerrit.wikimedia.org/g/mediawiki/extensions/WikiLove/+/93b9281a3f7f4d270cf510a3f28a48a6a6404d63/resources/ext.wikiLove.startup/WikiLoveDialog.vue#154
It's not safe to perform string replacements on HTML, especially when inserting another HTML element.

https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/extensions/WikiLove/+/93b9281a3f7f4d270cf510a3f28a48a6a6404d63/resources/ext.wikiLove.startup/wikiLove.js#69
https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/extensions/WikiLove/+/93b9281a3f7f4d270cf510a3f28a48a6a6404d63/resources/ext.wikiLove.startup/wikiLove.js#73
The URL protocol is not validated.

Additional information

MW: 1.46.0-alpha (2633444)
WikiLove: 1.3.1 (**93b9281**)

Details

Risk Rating
Medium

Author Affiliation
Wikimedia Communities

RELATED CHANGES IN GERRIT:

	Subject	Repo
	SECURITY: Sanitize URLs and use jQuery to build links	mediawiki/extensions/WikiLove
	SECURITY: Sanitize URLs and use jQuery to build links	mediawiki/extensions/WikiLove
	SECURITY: Sanitize URLs and use jQuery to build links	mediawiki/extensions/WikiLove
	SECURITY: Sanitize URLs and use jQuery to build links	mediawiki/extensions/WikiLove

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
rEWLO93b9281a3f7f: build: Updating lodash to 4.17.23

SomeRandomDeveloper created this task. 2026-02-04 17:45:40 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2026-02-04 17:45:42 (UTC+0)

SomeRandomDeveloper claimed this task. 2026-02-04 17:46:02 (UTC+0)

SomeRandomDeveloper added projects: **WikiLove**, **Vuln-XSS**, **affects-Miraheze**.

SomeRandomDeveloper added a project: **Patch-For-Review**. 2026-02-04 17:51:17 (UTC+0)

T416502.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)**. 2026-02-04 17:52:37 (UTC+0)

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board.
2026-02-04 21:18:07 (UTC+0)

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

sbassett subscribed.

> In ~~**T416502#11584441**~~, **@SomeRandomDeveloper** wrote:
>
> ***T416502.patch*** *4 KB*
> *Download*

Patch looks fine to me. I think we can get this deployed to Wikimedia production during the ad-hoc security deployment window we have scheduled tomorrow (2026-02-04), after the late backport window.

sbassett changed the task status from *Open* to *In Progress*. 2026-02-04 21:18:32 (UTC+0)

sbassett triaged this task as *Medium* priority.

Mstyles added a subscriber: **Scott_French**. 2026-02-05 22:43:54 (UTC+0)

Mstyles subscribed. 2026-02-05 23:30:12 (UTC+0)

> In ~~**T416502#11585143**~~, **@sbassett** wrote:
>
> > In ~~**T416502#11584441**~~, **@SomeRandomDeveloper** wrote:
> >
> > ***T416502.patch*** *4 KB*
> > *Download*
>
> *Patch looks fine to me. I think we can get this deployed to Wikimedia production during the ad-hoc security deployment window we have scheduled tomorrow (2026-02-04), after the late backport window.*

Deployed

Mstyles moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board.
2026-02-05 23:35:11 (UTC+0)

SomeRandomDeveloper removed a project: **Patch-For-Review**. 2026-03-06 21:24:33 (UTC+0)

SomeRandomDeveloper added a subscriber: **gerritbot**. 2026-03-14 14:28:46 (UTC+0)

Change #1251947 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): 2026-03-14 14:29:53 (UTC+0)
[mediawiki/extensions/WikiLove@master] SECURITY: Sanitize URLs and use jQuery to build links

Change #1251949 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/WikiLove@REL1_45] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:32:40 (UTC+0)

Change #1251950 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/WikiLove@REL1_44] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:33:08 (UTC+0)

Change #1251952 had a related patch set uploaded (by SomeRandomDeveloper; author: SomeRandomDeveloper): [mediawiki/extensions/WikiLove@REL1_43] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:45:02 (UTC+0)

Change #1251947 **merged** by jenkins-bot: [mediawiki/extensions/WikiLove@master] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:45:55 (UTC+0)

Change #1251950 **merged** by jenkins-bot: [mediawiki/extensions/WikiLove@REL1_44] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:53:57 (UTC+0)

Change #1251949 **merged** by jenkins-bot: [mediawiki/extensions/WikiLove@REL1_45] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 14:54:11 (UTC+0)

Change #1251952 **merged** by jenkins-bot: [mediawiki/extensions/WikiLove@REL1_43] SECURITY: Sanitize URLs and use jQuery to build links 2026-03-14 15:00:27 (UTC+0)

SomeRandomDeveloper closed this task as *Resolved*. 2026-03-14 15:32:21 (UTC+0)

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

Mstyles renamed this task from *Stored XSS through system messages in WikiLove* to *CVE-2026-22711: Stored XSS through system messages in WikiLove*. 2026-04-07 18:40:30 (UTC+0)

sbassett changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2026-04-08 15:05:42 (UTC+0)

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

sbassett changed Risk Rating from N/A to Medium.

sbassett moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board.