Maniphest T419186 Create Task

CVE-2026-39936: Stored XSS in Score due to usage of non-reserved data attributes

Actions

Closed, Resolved Public SECURITY

Assigned To

S SomeRandomDeveloper

Authored By

S SomeRandomDeveloper
2026-03-06 00:16:44 (UTC+0)

Tags

Security-Team (Watching)

Security

MediaWiki-extensions-Score (Backlog)

Vuln-XSS

SecTeam-Processed (Completed)

Referenced Files

F72783349: image.png
2026-03-09 21:42:51 (UTC+0)

F72627684: T419186.patch
2026-03-06 00:23:09 (UTC+0)

F72627602: image.png
2026-03-06 00:16:45 (UTC+0)

F72627599: image.png
2026-03-06 00:16:45 (UTC+0)

Subscribers

Aklapper

ASanford-WMF

Bawolff

gerritbot

Lucas_Werkmeister_WMDE

Mstyles

Reedy

View All 9 Subscribers

Description

The Score extension stores URLs in non-reserved data attributes and uses them for HTML links without appropriate sanitization, allowing for stored XSS through user interaction.

Reproduction steps

To exploit this, we need to be able to insert an `<img>` tag directly into a custom HTML element we can control the data attributes of. Since image thumbnails are wrapped in elements we can't control, the most straightforward solution is to use an SVG generated by Scribunto instead, which returns a strip marker that represents an `<img>` tag.

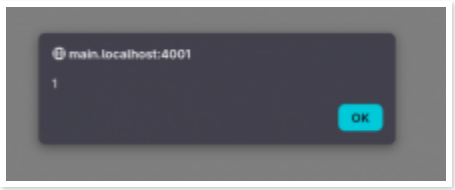
1. Create `Module:Svg` with the following code (it doesn't matter what kind of SVG it generates):

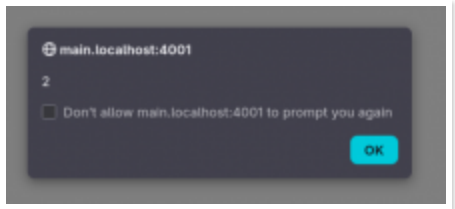
```
local p = {}

function p.generate()
  local svg = mw.svg.new()
  return svg:setAttribute( 'width', '120px' )
        :setAttribute( 'height', '120px' )
        :setContent( '<circle cx="50" cy="50" r="45" style="fill:green;" />' )
        :setImgAttribute( 'alt', 'SVG image' )
        :toImage()
end

return p
```

2. Create a new page with the following contents:

```
<score lang="lilypond">\relative c' { f d f a d f e d cis a cis e a g f e }</score>
<div class="mw-ext-score" data-midi="javascript:alert(1)" data-source="javascript:alert(2)">
{{#invoke:Svg|generate}}</div>
```

3. Visit the page and click on the green circle
4. Click on one of the two links in the popup





Cause

Non-reserved data attributes are used as the `href` attributes of two links:
https://github.com/wikimedia/mediawiki-extensions-Score/blob/979253d7583ddc82413c47e48c9d47fd8042d4d0/modules/ext.score.popup/popup.js#L4-L26

Additional information

MW 1.46.0-alpha (**d03de87**)
Score 0.3.0 (**979253d**)

Details

Author Affiliation
Wikimedia Communities

RELATED CHANGES IN GERRIT:

	Subject	Repo
	SECURITY: Use reserved data attributes to store URLs	mediawiki/extensions/Score
	SECURITY: Use reserved data attributes to store URLs	mediawiki/extensions/Score
	SECURITY: Use reserved data attributes to store URLs	mediawiki/extensions/Score
	SECURITY: Use reserved data attributes to store URLs	mediawiki/extensions/Score

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
rESCR979253d7583d: Localisation updates from https://translatewiki.net.
rMWd03de878205b: Language: Tiny clarity and perf improvement

SomeRandomDeveloper created this task. 2026-03-06 00:16:44 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2026-03-06 00:16:47 (UTC+0)

SomeRandomDeveloper claimed this task. 2026-03-06 00:17:04 (UTC+0)

SomeRandomDeveloper added projects: **MediaWiki-extensions-Score**, **Vuln-XSS**.

SomeRandomDeveloper added a project: **Patch-For-Review**. 2026-03-06 00:23:09 (UTC+0)

Suggested patch:

T419186.patch 1 KB
Download

(Note that I don't have shellbox/lilypond set up locally right now, so I can't test it properly, but it should definitely fix the XSS)

Bawolff subscribed. 2026-03-06 02:40:41 (UTC+0)

That's a nice find.

Another example of an XSS that would be prevented with a proper CSP policy.

Lucas_Werkmeister_WMDE subscribed. Edited · 2026-03-06 11:33:38 (UTC+0)

I have a working Score setup and can confirm that the patch fixes the stored XSS. The popup on the SVG stops appearing as soon as the new SVG is loaded, though the popup on scores is broken until the pages are purged (so the `data-*` attributes in the parser cache turn into `data-mw-*` attributes). CR+1, should be okay to deploy and then ideally purge the affected pages at least on major wikis (e.g. `action=purge` + `generator=categorymembers` + `gcmtitle=Category:Pages using the Score extension` + `gcmlimit=max`, then sleep and follow continuation until done; category name varies by wiki).

Edit: (I probably meant “The popup on the SVG stops appearing as soon as the new *JS* is loaded”, oops.)

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)**. 2026-03-06 21:07:28 (UTC+0)

sbassett moved this task from **Incoming** to **Security Patch To Deploy** on the **Security-Team** board. 2026-03-09 17:30:43 (UTC+0)

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

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

cc: **@Mstyles**

ASanford-WMF subscribed. 2026-03-09 21:32:01 (UTC+0)

Deployed - https://sal.toolforge.org/log/b2iB1JwBffdvpiTriF48

@SomeRandomDeveloper could you test this to make sure the patch is working in production?

ASanford-WMF moved this task from **Security Patch To Deploy** to **Watching** on the **Security-Team** board.
2026-03-09 21:32:52 (UTC+0)

ASanford-WMF removed a project: **Patch-For-Review**.

SomeRandomDeveloper added a comment. 2026-03-09 21:42:51 (UTC+0)

I went to https://en.wikipedia.org/wiki/Special:ExpandTemplates?wpInput=%3Cscore%20lang%3D%22lilypond%22%3E%5Crelative%20c'%20%7B%20f%20d%20f%20a%20d%20f%20e%20d%20cis%20a%20cis%20e%20a%20g%20f%20e%20%7D%3C%2Fscore%3E and the emitted HTML still contains the `data-midi` attribute:

Since my patch changes it to `data-mw-midi`, and I don't think anything on the PHP side should be caching the attribute, it doesn't seem to me that the patch was applied properly

sbassett added a comment. 2026-03-09 21:48:18 (UTC+0)

> In ~~**T419186#11690200**~~, **@SomeRandomDeveloper** wrote:
>
> *I went to https://en.wikipedia.org/wiki/Special:ExpandTemplates?wpInput=%3Cscore%20lang%3D%22lilypond%22%3E%5Crelative%20c'%20%7B%20f%20d%20f%20a%20d%20f%20e%20d%20cis%20a%20cis%20e%20a%20g%20f%20e%20%7D%3C%2Fscore%3E and the emitted HTML still contains the `data-midi` attribute:*
>
> 
>
> *Since my patch changes it to `data-mw-midi`, and I don't think anything on the PHP side should be caching the attribute, it doesn't seem to me that the patch was applied properly*

Yes, this appears to be the case. We are investigating this now. Please bear with us as we are working to train up some other folks on the Wikimedia production security deployment process.

ASanford-WMF added a comment. 2026-03-09 22:03:26 (UTC+0)

@SomeRandomDeveloper Sorry about that! This should be deployed now - https://sal.toolforge.org/log/DGif1JwBffdvpiTrkH7z

It looks like the `data-mw-wiki` attribute is on the element now. Could you confirm?

SomeRandomDeveloper added a comment. 2026-03-09 23:06:33 (UTC+0)

> In ~~T419186#11690242~~, @**ASanford-WMF** wrote:
>
> *@SomeRandomDeveloper Sorry about that! This should be deployed now - https://sal.toolforge.org/log/DGif1JwBffdvpiTrkH7z*
>
> *It looks like the `data-mw-wiki` attribute is on the element now. Could you confirm?*

No worries; yes, it looks fine to me now.

Reedy added subscribers: **gerritbot**, **Reedy**. 2026-04-01 13:05:28 (UTC+0)

Any objections for this patch to go through Gerrit?

sbassett added a comment. 2026-04-01 14:40:52 (UTC+0)

> In ~~T419186#11777816~~, @**Reedy** wrote:
>
> *Any objections for this patch to go through Gerrit?*

Not from me.

Change #1267097 had a related patch set uploaded (by Reedy; author: SomeRandomDeveloper): 2026-04-02 15:46:53 (UTC+0)
[mediawiki/extensions/Score@master] SECURITY: Use reserved data attributes to store URLs

Change #1267097 **merged** by jenkins-bot: 2026-04-02 15:59:16 (UTC+0)
[mediawiki/extensions/Score@master] SECURITY: Use reserved data attributes to store URLs

Change #1267103 had a related patch set uploaded (by Reedy; author: SomeRandomDeveloper): 2026-04-02 15:59:31 (UTC+0)
[mediawiki/extensions/Score@REL1_45] SECURITY: Use reserved data attributes to store URLs

Change #1267105 had a related patch set uploaded (by Reedy; author: SomeRandomDeveloper): 2026-04-02 15:59:47 (UTC+0)
[mediawiki/extensions/Score@REL1_44] SECURITY: Use reserved data attributes to store URLs

Change #1267106 had a related patch set uploaded (by Reedy; author: SomeRandomDeveloper): 2026-04-02 16:00:04 (UTC+0)
[mediawiki/extensions/Score@REL1_43] SECURITY: Use reserved data attributes to store URLs

Change #1267103 **merged** by jenkins-bot: 2026-04-02 16:23:56 (UTC+0)
[mediawiki/extensions/Score@REL1_45] SECURITY: Use reserved data attributes to store URLs

Change #1267106 **merged** by jenkins-bot: 2026-04-02 16:41:07 (UTC+0)
[mediawiki/extensions/Score@REL1_43] SECURITY: Use reserved data attributes to store URLs

Change #1267105 **merged** by jenkins-bot: 2026-04-02 18:10:59 (UTC+0)
[mediawiki/extensions/Score@REL1_44] SECURITY: Use reserved data attributes to store URLs

Mstyles renamed this task from *Stored XSS in Score due to usage of non-reserved data attributes* to *CVE-2026-39936: Stored XSS in Score due to usage of non-reserved data attributes*. 2026-04-07 22:30:59 (UTC+0)

Mstyles closed this task as *Resolved*.

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

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

A_smart_kitten removed a project: **Patch-For-Review**. 2026-04-08 09:39:51 (UTC+0)