

🔍 makeCollapsible allows applying event handler to any CSS selector (CVE-2020-10960)

🔒 Closed, Resolved🌐 PublicSECURITY

≡ Actions

Assigned To

sbassett

Authored By

Yair_rand

2020-03-02 03:28:24 (UTC+0)

Tags

👤 Security-Team (In Progress)

👤 Security

👤 MediaWiki-General

👤 MW-1.31-release-notes

👤 MW-1.34-notes

👤 MW-1.33-notes

📌 MW-1.35-notes (1.35.0-wmf.26; 2020-03-31)

Referenced Files

📄 F31655696: 0001-jquery.makeCollapsible-Escape-user-generated-CSS-sel.patch

2020-03-02 16:12:36 (UTC+0)

Subscribers

Aklapper

Danny5712

matmarex

Reedy

Yair_rand

Tokens

Description

The code `a`, when placed on a wiki page, causes the `body` element to undergo several changes: It has the `mw-customtoggle` class and `tabindex=0` applied to it, along with several event handlers being attached which collapse or expand a particular element (many of these handlers suppressing normal behaviour). The "body" can be replaced with any CSS selector, including, for example " * ", which will then have the effects apply to all elements matching the selector.

The source of this is presumably [https://phabricator.wikimedia.org/source/mediawiki/browse/master/resources/src/jquery/jquery.makeCollapsible.js\\$246](https://phabricator.wikimedia.org/source/mediawiki/browse/master/resources/src/jquery/jquery.makeCollapsible.js$246)

(I don't think this bug matters much on its own, but I'm a bit concerned about what bugs this could be combined with to open up some worrisome possibilities. Sorry if this isn't the kind of thing that should be labelled a security issue, I'm not sure what the boundaries are.)

Details

Project	Subject
mediawiki/core	SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
mediawiki/core	SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
mediawiki/core	SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
mediawiki/core	SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors

Customize query in [gerit](#)

Related Objects

🔍 Search... ▼

Task	Graph	Mentions
Status	Assigned	Task
🔒 Resolved	Reedy	🔒240392 Release MediaWiki 1.31.7/1.33.3/1.34.1
🌐 Resolved	Reedy	🔒240393 Tracking bug for MediaWiki 1.31.7/1.33.3/1.34.1
🔒 Resolved	sbassett	🔒246602 makeCollapsible allows applying event handler to any CSS selector (CVE-2020-10960)

- 🔧 Yair_rand created this task. 2020-03-02 03:28:24 (UTC+0)
- 👤 [Restricted Application](#) added a subscriber: [Aklapper](#). · [View Herald Transcript](#) 2020-03-02 03:28:26 (UTC+0)
- 🔗 [Aklapper](#) added a project: [MediaWiki-General](#). 2020-03-02 09:42:02 (UTC+0)


👤 [matmarex](#) added a subscriber: [matmarex](#). 2020-03-02 16:12:36 (UTC+0)

Thanks for reporting this. You can use security issues for anything even slightly concerning that you don't want to make public.

Note that you need to use `$wgFragmentMode = ['html5', 'legacy']`; (or similar) to reproduce this, by default MediaWiki escapes ID attributes in a manner that breaks this. We use this config on Wikimedia sites though.

I don't think this can result in anything *really* scary like an XSS problem. It allows the content of the page to affect the MediaWiki interface, which is bad since it can often interfere with the admins' ability to revert the edit or delete the page, but in this case I couldn't find a way to do anything other than make clicks anywhere on the page hide/show a part of the content. We just got lucky though.

Potential fix is to use `$.escapeSelector` :

 **0001-jquery.makeCollapsible-Escape-user-generated-CSS-sel.patch** 1 KB
Download

- **chasemp** assigned this task to **sbassett**. 2020-03-02 16:36:15 (UTC+0)
- • **chasemp** triaged this task as *Low* priority.
- 📋 • **chasemp** moved this task from *Incoming* to *In Progress* on the **Security-Team** board.

💬 **sbassett** added a comment. 2020-03-02 22:50:59 (UTC+0)


In ~~T246602#5933105~~, @matmarex wrote:

Note that you need to use `$wgFragmentMode = ['html5', 'legacy']`; (or similar) to reproduce this, by default MediaWiki escapes ID attributes in a manner that breaks this. We use this config on Wikimedia sites though.

It wasn't immediately clear to me, but the order of the array values appears to matter. When `$wgFragmentMode` is set to `['legacy', 'html5']` (its default), it defangs the bad id whereas setting it to `['html5', 'legacy']` or `['html5']` does not.

I don't think this can result in anything really scary like an XSS problem. It allows the content of the page to affect the MediaWiki interface, which is bad since it can often interfere with the admins' ability to revert the edit or delete the page, but in this case I couldn't find a way to do anything other than make clicks anywhere on the page hide/show a part of the content. We just got lucky though.

Potential fix is to use `$.escapeSelector` :

 **0001-jquery.makeCollapsible-Escape-user-generated-CSS-sel.patch** 1 KB
Download

I'd agree that this would likely be difficult to exploit in any serious way, though we did just have a different UI issue with security implications (~~T232932~~). Patch looks good and tests fine. I think I'm going to deploy it now during the remainder of the weekly security deployment window.

💬 **sbassett** added a comment. 2020-03-02 23:21:14 (UTC+0)

Deployed to wmf.21. Seems fine on testwiki.

🔗 **sbassett** added a parent task: ~~T240393-Tracking bug for MediaWiki 1.34.7/1.33.3/1.34.4~~. 2020-03-02 23:25:10 (UTC+0)

🔗 **sbassett** mentioned this in ~~T240393-Tracking bug for MediaWiki 1.34.7/1.33.3/1.34.4~~.

👤 **Krinkle** awarded a token. 2020-03-05 02:46:27 (UTC+0)

✅ **Reedy** closed this task as *Resolved*. 2020-03-24 17:13:42 (UTC+0)

👤 **Reedy** added a subscriber: **Reedy**.

Patch applies cleanly to master, REL1_34, REL1_33 and REL1_31. Closing as release is coming this week

✍️ **sbassett** renamed this task from *makeCollapsible allows applying event handler to any CSS selector* to *makeCollapsible allows applying event handler to any CSS selector (CVE-2020-10960)*. 2020-03-26 03:40:31 (UTC+0)

🔗 **sbassett** mentioned this in ~~T240393-Obtain CVEs for 1.31.7/1.33.3/1.34.4 security releases~~.

🔒 **Reedy** changed the visibility from *"Custom Policy"* to *"Public (No Login Required)"*. 2020-03-26 17:42:04 (UTC+0)

💬 **gerritbot** added a comment. 2020-03-26 17:42:12 (UTC+0)

Change 583697 **merged** by jenkins-bot:
[mediawiki/core@REL1_31] SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
<https://gerrit.wikimedia.org/r/583697>

💬 **gerritbot** added a comment. 2020-03-26 17:46:06 (UTC+0)

Change 583700 **merged** by jenkins-bot:
[mediawiki/core@REL1_33] SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
<https://gerrit.wikimedia.org/r/583700>

💬 **gerritbot** added a comment. 2020-03-26 17:47:47 (UTC+0)

Change 583703 **merged** by jenkins-bot:
[mediawiki/core@REL1_34] SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
<https://gerrit.wikimedia.org/r/583703>

👤 **DannyS712** added a subscriber: **DannyS712**. 2020-03-26 17:52:51 (UTC+0)

💬 **gerritbot** added a comment. 2020-03-26 17:57:00 (UTC+0)

Change 583708 **merged** by jenkins-bot:
[mediawiki/core@master] SECURITY: jquery.makeCollapsible: Escape user-generated CSS selectors
<https://gerrit.wikimedia.org/r/583708>

🔗 **Jdforrester-WMF** added projects: ~~MW 1.31 release notes~~, ~~MW 1.34 notes~~, ~~MW 1.33 notes~~. 2020-03-27 17:33:40 (UTC+0)

🔗 **Jdforrester-WMF** added a project: ~~MW 1.35 notes (1.35.0 wmf.26; 2020-03-31)~~.