

CVE-2021-30157: Unescaped messages used in HTML on ChangesList pages (e.g. RecentChanges and Watchlist)

Closed, Resolved

Public

SECURITY

Actions

Assigned To

Grunny

Authored By

Grunny

2021-03-21 18:00:40 (UTC+0)

Tags

Security-Team

 (In Progress)

Security

Vuln-XSS

MediaWiki-Special-pages

 (To triage)

MW-1.31-release

 (Backlog)

MW-1.35-release

 (Blocker)

SecTeam-Processed

MW-1.36-notes

MW-1.35-notes

MW-1.31-release-notes

Referenced Files

F34176672: T278058.patch

2021-03-21 18:06:43 (UTC+0)

F34176654: RecentChangesXSS.png

2021-03-21 18:00:40 (UTC+0)

Subscribers

Aklapper

Catrope

gerritbot

Grunny

RhinosF1

sbassett

Description

On ChangesList special pages like Special:RecentChanges and Special:Watchlist, some of the `rcfilters-filter-*` label messages are output in HTML unescaped.

Steps to reproduce:

1. Edit one of the `rcfilters-filter-*`-label messages (e.g. `edit MediaWiki:Rcfilters-filter-humans-label`) and add a simple XSS string like `<img src=x onerror=alert(document.domain)>`




2. Visit Special:RecentChanges and see the JavaScript executed (depending on which label you chose in step 1, you may need to select that filter in the interface or URL param first)



This happens because the label is being added by JS using `append` in this case, when the message itself is unescaped plain text. This appears to have been the case since `<> https://phabricator.wikimedia.org/rMWd0339e8741fb0a8361aed563b92f3fd36fdb3f7b` where the label was previously always wrapped in `mw.html.escape` but afterwards was output raw if there isn't a wrapping label message.

It's relatively low risk given it's admin-only, but filing as a private issue similar to `T256171`, `T255918` and `T278014`.

Details


Project	Subject
 mediawiki/core	Escape <code>rcfilters-filter-*</code> messages on ChangesList pages
 mediawiki/core	Escape <code>rcfilters-filter-*</code> messages on ChangesList pages
 mediawiki/core	Escape <code>rcfilters-filter-*</code> messages on ChangesList pages


Customize query in Gerrit


Related Objects


Search...

Task Graph	Mentions	
Status	Assigned	Task
 Resolved	Reedy	<del>T270458</del> Release MediaWiki 1.31.13/1.35.2
 Resolved	Reedy	<del>T270459</del> Tracking bug for MediaWiki 1.31.13/1.35.2
 Open	None	T2212 <a href="#">Some MediaWiki: messages not safe in HTML (tracking)</a>
 Resolved	Grunny	<del>T278058</del> CVE-2021-30157: Unescaped messages used in HTML on ChangesList pages (e.g. RecentChanges and Watchlist)

 Grunny created this task. 2021-03-21 18:00:40 (UTC+0)

- 

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-03-21 18:00:42 (UTC+0)
- 

Grunny added a parent task: **T2212: Some MediaWiki: messages not safe in HTML (tracking)**. 2021-03-21 18:01:05 (UTC+0)
- 

Grunny added projects: **Vuln-XSS, MediaWiki-Special-pages**.



Grunny added a comment. 2021-03-21 18:06:43 (UTC+0)

Proposed patch:

 **T278058.patch** 1 KB

Download


From 60be0e4cdf37fce9a83d9df0bd1497107bc5f940 Mon Sep 17 00:00:00 2001  
From: grunny <mwgrunny@gmail.com>  
Date: Sun, 21 Mar 2021 14:35:58 +1000  
Subject: [PATCH] Escape rcfilters-filter-\* messages on ChangesList pages


The rcfilters-filter-\* label messages are output as raw HTML on ChangesList pages like RecentChanges and Watchlist. If there is a wrapping label message, the label is properly escaped, but when there is not, it is appended as raw HTML. This escapes the label at output by switching to .text().

Change-Id: I7106aedced51343439fc54d5bb91620d8a0362f9  
---  
resources/src/mediawiki.rcfilters/ui/TagItemWidget.js | 2 +-  
1 file changed, 1 insertion(+), 1 deletion(-)


```
diff --git a/resources/src/mediawiki.rcfilters/ui/TagItemWidget.js b/resources/src/mediawiki.rcfilters/ui/TagItemWidget.js
index 5d45d18..ba7b920 100644
--- a/resources/src/mediawiki.rcfilters/ui/TagItemWidget.js
+++ b/resources/src/mediawiki.rcfilters/ui/TagItemWidget.js
@@ -94,7 +94,7 @@ TagItemWidget.prototype.updateUiBasedOnState = function () {
    ).contents() );
    } else {
        this.setLabel(
-            $( '<bdi>' ).append(
+            $( '<bdi>' ).text(
                this.itemModel.getLabel()
            )
        );
    }
}
```

--  
2.7.4

- 


Legoktm added a subscriber: **Catrope**. 2021-03-22 06:31:05 (UTC+0)
- 


Reedy added projects: **MW-1.34-release, MW-1.35-release**. 2021-03-22 15:14:33 (UTC+0)





sbassett added a subscriber: **sbassett**. 2021-03-22 15:36:12 (UTC+0)


Thanks again for the report and patch. Making this public and pushing through gerrit as low-risk.

- 

sbassett triaged this task as **Low** priority. 2021-03-22 15:36:30 (UTC+0)
- 


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

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

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

sbassett moved this task from **Incoming** to **In Progress** on the **Security-Team** board.
- 

RhinosF1 added a subscriber: **RhinosF1**. 2021-03-22 15:37:26 (UTC+0)



gerritbot added a comment. 2021-03-22 15:39:52 (UTC+0)

Change 674085 had a related patch set uploaded (by SBassett; owner: Grunny):  
[mediawiki/core@master] Escape rcfilters-filter-\* messages on ChangesList pages  
<https://gerrit.wikimedia.org/r/674085>



gerritbot added a project: **Patch-For-Review**. 2021-03-22 15:39:53 (UTC+0)



gerritbot added a comment. 2021-03-22 19:18:52 (UTC+0)

Change 674085 **merged** by jenkins-bot:  
[mediawiki/core@master] Escape rcfilters-filter-\* messages on ChangesList pages  
<https://gerrit.wikimedia.org/r/674085>



gerritbot added a comment. 2021-03-22 19:49:03 (UTC+0)

Change 674108 had a related patch set uploaded (by SBassett; owner: Grunny):  
[mediawiki/core@REL1\_35] Escape rcfilters-filter-\* messages on ChangesList pages  
<https://gerrit.wikimedia.org/r/674108>



ReleaseTaggerBot added a project: **MW-1.36-notes (1.36.0 wmf.36, 2021-03-23)**. 2021-03-22 20:00:30 (UTC+0)



gerritbot added a comment. 2021-03-22 20:12:30 (UTC+0)

Change 674108 **merged** by jenkins-bot:  
[mediawiki/core@REL1\_35] Escape rcfilters-filter-\* messages on ChangesList pages  
<https://gerrit.wikimedia.org/r/674108>



gerritbot added a comment. 2021-03-22 20:21:35 (UTC+0)

Change 674110 had a related patch set uploaded (by Reedy; owner: Grunny):  
[mediawiki/core@REL1\_31] Escape rcfilters-filter-\* messages on ChangesList pages

 **ReleaseTaggerBot** added a project: **MW-1.35-notes**. 2021-03-22 21:00:27 (UTC+0)

 **gerritbot** added a comment. 2021-03-23 18:38:58 (UTC+0)


Change 674110 **merged** by jenkins-bot:  
[mediawiki/core@REL1\_31] Escape rcfilters-filter-\* messages on ChangesList pages

<https://gerrit.wikimedia.org/r/674110>

 **ReleaseTaggerBot** added a project: ~~MW-1.34-release-notes~~. 2021-03-23 19:00:30 (UTC+0)

 **Maintenance\_bot** removed a project: **Patch-For-Review**. 2021-03-23 19:11:14 (UTC+0)

 **Reedy** closed this task as *Resolved*. 2021-03-30 00:44:08 (UTC+0)

 **Reedy** assigned this task to **Grunny**.

 **Reedy** added a parent task: ~~T270459: Tracking bug for MediaWiki 1.34.13/1.35.2.~~

 **Reedy** mentioned this in ~~T270459: Tracking bug for MediaWiki 1.34.13/1.35.2.~~

 **Reedy** renamed this task from *Unescaped messages used in HTML on ChangesList pages (e.g. RecentChanges and Watchlist)* to *CVE-2021-30157: Unescaped messages used in HTML on ChangesList pages (e.g. RecentChanges and Watchlist)*.  
2021-04-06 19:13:15 (UTC+0)

 **Reedy** added a subscriber: **gerritbot**. 2021-04-08 19:11:23 (UTC+0)

 **matmarex** mentioned this in ~~T281595: XSS from not escaping HTML messages in recent core patch.~~ 2021-04-30 18:57:17 (UTC+0)