Message recentchanges-legend-watchlistexpiry can contain raw html (CVE-2020-35474)

Closed, Resolved · Public · SECURITY

Actions

Assigned To

Umherirrender

Authored By

Umherirrender
2020-11-27 19:03:01 (UTC+0)

Tags

Security-Team (Watching)
Security
Vuln-XSS
Expiring-Watchlist-Items (Backlog)
Community-Tech (New & TBD Tickets)
MW-1.36-notes (1.36.0-wmf.21; 2020-12-08)
MW-1.31-release-notes
MW-1.35-notes

Referenced Files

None

Subscribers

Aklapper
gerritbot
Reedy
sbassett
Umherirrender

Description

While working on ~~T216348~~ I have found an issue with message `recentchanges-legend-watchlistexpiry`

Added with https://gerrit.wikimedia.org/r/c/mediawiki/core/+/596540/21/includes/specialpage/ChangesListSpecialPage.php

```
$legend .= Html::rawElement(
        'dd',
        [ 'class' => 'mw-changeslist-legend-watchlistexpiry', 'id' => $watchlistLabelId ],
        $context->msg( 'recentchanges-legend-watchlistexpiry' )->text()
);
```

The combination of `Html::rawElement` and `Message::text` leads to XSS leaks

The message was added with 1.35 and is behind a feature flag (`$wgWatchlistExpiry`)

Should use `Html::element` or `Message::parse` / `Message::escaped` , not sure.

Details

	Project	Subject
	mediawiki/core	Use Html::element in ChangeListSpecialPage for sanity
	mediawiki/core	Use Html::element in ChangeListSpecialPage for sanity
	mediawiki/core	Use Html::element in ChangeListSpecialPage for sanity

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

Status	Assigned	Task
Resolved	Reedy	~~T263802~~ Release MediaWiki 1.31.11/1.35.1
Resolved	Reedy	~~T263803~~ Tracking bug for MediaWiki 1.31.11/1.35.1
Resolved	Umherirrender	~~T268894~~ Message recentchanges-legend-watchlistexpiry can contain raw html (CVE-2020-35474)

Umherirrender created this task. 2020-11-27 19:03:01 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2020-11-27 19:03:03 (UTC+0)

Daimona added a project: **Vuln-XSS**. 2020-11-27 22:56:50 (UTC+0)

Aklapper added a project: **Expiring-Watchlist-Items**. 2020-11-28 14:56:02 (UTC+0)

Restricted Application added a project: **Community-Tech**. · View Herald Transcript 2020-11-28 14:56:04 (UTC+0)

sbassett triaged this task as *High* priority. 2020-11-30 16:23:05 (UTC+0)

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

sbassett added a subscriber: **sbassett**. Edited · 2020-11-30 16:52:57 (UTC+0)

> *Should use Html::element or Message::parse/Message::escaped, not sure.*

`->escaped()` is probably the easier fix. Also, IMO this should be low-risk enough (given the current messages) that it could be done publicly through gerrit with a benign commit message signaling that it's code-hardening.

sbassett mentioned this in ~~**T268917: Messages userrights-expiry-current and userrights-expiry-none can contain raw html (CVE-2020-35475)**~~. 2020-11-30 16:55:53 (UTC+0)

Umherirrender claimed this task. 2020-12-07 16:51:26 (UTC+0)

Fixed with https://gerrit.wikimedia.org/r/c/mediawiki/core/+/646676

Could be public from my point of view

sbassett added a comment. 2020-12-07 16:58:58 (UTC+0)

> In ~~**T268894#6673740**~~, **@Umherirrender** wrote:
> *Could be public from my point of view*

Similar to ~~**T268917**~~, let's wait for the train deployments this week and then make this task public.

sbassett added a parent task: ~~**T263003: Tracking bug for MediaWiki 1.31.11/1.35.1**~~. 2020-12-07 17:07:00 (UTC+0)

Jdforrester-WMF added a project: ~~**MW-1.36-notes (1.36.0-wmf.21; 2020-12-08)**~~. 2020-12-07 17:21:44 (UTC+0)

Reedy added a subscriber: **gerritbot**. 2020-12-15 13:10:43 (UTC+0)

gerritbot added a comment. 2020-12-15 13:22:44 (UTC+0)

Change 649517 **merged** by jenkins-bot:
[mediawiki/core@REL1_35] Use Html::element in ChangeListSpecialPage for sanity

https://gerrit.wikimedia.org/r/649517

Reedy closed this task as *Resolved*. 2020-12-15 13:23:11 (UTC+0)

Reedy added a subscriber: **Reedy**.

Closing for ease of tracking. Can/will be made public later

Reedy mentioned this in ~~**T263003: Tracking bug for MediaWiki 1.31.11/1.35.1**~~. 2020-12-15 13:24:08 (UTC+0)

Reedy mentioned this in ~~**T263009: Obtain CVEs for 1.31.11/1.35.1 security releases**~~. 2020-12-15 14:03:31 (UTC+0)

Jdforrester-WMF added projects: ~~**MW-1.31-release-notes**~~, **MW-1.35-notes**. 2020-12-15 16:36:19 (UTC+0)

Reedy renamed this task from *Message recentchanges-legend-watchlistexpiry can contain raw html* to *Message recentchanges-legend-watchlistexpiry can contain raw html (CVE-2020-35474)*. 2020-12-16 12:35:21 (UTC+0)

Reedy changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2020-12-18 00:24:02 (UTC+0)

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