CVE-2021-30154: Unescaped messages used in HTML on Special:NewFiles

Closed, Resolved · Public · SECURITY

Actions

Assigned To

Grunny

Authored By

Grunny
2021-03-20 15:59:19 (UTC+0)

Tags

Security-Team (Our Part Is Done)
Security
Vuln-XSS
MediaWiki-Special-pages (To triage)
MW-1.35-release (Blocker)
SecTeam-Processed (Completed)
MW-1.36-notes (1.36.0-wmf.36; 2021-03-23)
MW-1.35-notes
MW-1.31-release (Backlog)
MW-1.31-release-notes

Referenced Files

F34176637: T278014.patch
2021-03-21 17:35:00 (UTC+0)

F34175119: NewFilesXSS.png
2021-03-20 15:59:19 (UTC+0)

Subscribers

Aklapper
gerritbot
Grunny
matthiasmullie
Reedy
RhinosF1
sbassett

Description

On Special:NewFiles, all the `mediastatistics-header-*` messages are output in HTML unescaped.

Steps to reproduce:

1. Edit one of the `mediastatistics-header-*` messages (e.g. edit `MediaWiki:Mediastatistics-header-drawing`) and add a simple XSS string like `<img src=x onerror=alert(document.domain)>`
2. Visit Special:NewFiles and see the JavaScript executed

This happens because the form options is using the `->text()` output format with `options`, which is not escaped, rather than `options-messages`.

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

Details

Author Affiliation
Wikimedia Communities

	Project	Subject
	mediawiki/core	Escape mediastatistics-header-* messages on Special:NewFiles
	mediawiki/core	Escape mediastatistics-header-* messages on Special:NewFiles
	mediawiki/core	Escape mediastatistics-header-* messages on Special:NewFiles

Customize query in gerrit

Related Objects

Search...

Task Graph | Mentions

Status	Assigned	Task
Resolved	Reedy	~~T270458~~ Release MediaWiki 1.31.13/1.35.2
Resolved	Reedy	~~T270459~~ Tracking bug for MediaWiki 1.31.13/1.35.2
Open	*None*	T2212 Some MediaWiki: messages not safe in HTML (tracking)

Resolved Grunny ~~T278014~~ **CVE-2021-30154: Unescaped messages used in HTML on Special:NewFiles**

Grunny created this task. 2021-03-20 15:59:19 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2021-03-20 15:59:20 (UTC+0)

Grunny added a comment. Edited · 2021-03-20 16:02:06 (UTC+0)

Proposed patch:

T278014.patch 1 KB
Download

```
From 65b0d900790a2fc8b96007425ac9aa850e9fd6dd Mon Sep 17 00:00:00 2001
From: grunny <mwgrunny@gmail.com>
Date: Sat, 20 Mar 2021 04:46:44 +1000
Subject: [PATCH] Escape mediastatistics-header-* messages on Special:NewFiles

The mediastatistics-header-* messages used on Special:NewFiles currently
allow raw HTML as raw options labels are output as raw HTML in forms. We
could change these to use options-messages with the message keys, but it
looks like this was done so the list could be alphabetised based on the
labels and this wouldn't be in alphabetical order if we sorted on the
message keys.

Change-Id: I5f59ccf4c167756255952cfbf31a8d7891463e92
---
 includes/specials/SpecialNewFiles.php | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/includes/specials/SpecialNewFiles.php b/includes/specials/SpecialNewFiles.php
index fc589f1..92798e0 100644
--- a/includes/specials/SpecialNewFiles.php
+++ b/includes/specials/SpecialNewFiles.php
@@ -155,7 +155,7 @@ class SpecialNewFiles extends IncludableSpecialPage {
                        // mediastatistics-header-office, mediastatistics-header-text,
                        // mediastatistics-header-executable, mediastatistics-header-archive,
                        // mediastatistics-header-3d,
-                       return $this->msg( 'mediastatistics-header-' . strtolower( $type ) )->text();
+                       return $this->msg( 'mediastatistics-header-' . strtolower( $type ) )->escaped();
                }, $this->mediaTypes );
                $mediaTypesOptions = array_combine( $mediaTypesText, $this->mediaTypes );
                ksort( $mediaTypesOptions );
--
2.7.4
```

As the commit message says, we could use options-messages, but it seems this was intended to allow the output list to be alphabetical, which this approach maintains.

Grunny added a parent task: **T2212: Some MediaWiki: messages not safe in HTML (tracking)**. 2021-03-20 16:03:41 (UTC+0)

Grunny added a project: **Vuln-XSS**. 2021-03-20 16:08:22 (UTC+0)

Reedy added a project: **MediaWiki-Special-pages**. 2021-03-20 17:38:22 (UTC+0)

Reedy added a project: **MW-1.35-release**. 2021-03-20 17:44:03 (UTC+0)

Reedy added subscribers: **matthiasmullie**, **Reedy**.

Thanks Grunny.

Seems this might have been the case since **rMW2647cbc4a456: Add media type based filtering to Special:NewFiles**

Grunny mentioned this in ~~**T278050: CVE-2021-30157: Unescaped messages used in HTML on ChangesList pages (e.g. RecentChanges and Watchlist)**~~. 2021-03-21 18:00:40 (UTC+0)

sbassett triaged this task as *Low* priority. 2021-03-22 15:25:35 (UTC+0)

sbassett changed Author Affiliation from N/A to Wikimedia Communities.

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.

sbassett added a subscriber: **sbassett**.

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

RhinosF1 added a subscriber: **RhinosF1**. 2021-03-22 15:27:41 (UTC+0)

gerritbot added a comment. 2021-03-22 15:30:33 (UTC+0)

Change 674083 had a related patch set uploaded (by SBassett; owner: Grunny):
[mediawiki/core@master] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/674083

gerritbot added a project: **Patch-For-Review**. 2021-03-22 15:30:33 (UTC+0)

sbassett added a project: **SecTeam-Processed**. 2021-03-22 15:40:47 (UTC+0)

gerritbot added a comment. 2021-03-22 17:23:03 (UTC+0)

Change 674083 **merged** by jenkins-bot:
[mediawiki/core@master] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/674083

gerritbot added a comment. 2021-03-22 17:46:26 (UTC+0)

Change 674107 had a related patch set uploaded (by SBassett; owner: Grunny):
[mediawiki/core@REL1_35] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/674107

Grunny added a comment. 2021-03-22 17:59:19 (UTC+0)

Thanks, @sbassett ! Just for my reference on if I find any more of these in core or WMF deployed extensions, is it OK to push straight to Gerrit, and I assume we'd still want a ticket created for reference?

gerritbot added a comment. 2021-03-22 18:00:05 (UTC+0)

Change 674107 **merged** by jenkins-bot:
[mediawiki/core@REL1_35] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/674107

ReleaseTaggerBot added projects: ~~**MW-1.36-notes (1.36.0-wmf.36; 2021-03-23)**~~, **MW-1.35-notes**. 2021-03-22 18:00:30 (UTC+0)

sbassett added a comment. 2021-03-22 18:06:49 (UTC+0)

> In ~~**T278014#6935629**~~, **@Grunny** wrote:
> *Thanks, @sbassett ! Just for my reference on if I find any more of these in core or WMF deployed extensions, is it OK to push straight to Gerrit, and I assume we'd still want a ticket created for reference?*

I would say likely, yes. However it's probably a good idea to continue filing these as private bugs so the Security-Team can review them (our weekly clinic meeting is Monday morning) just to verify they are indeed low-risk and to also time them well for the weekly train deployment, in getting pushed to gerrit.

sbassett moved this task from **In Progress** to **Our Part Is Done** on the **Security-Team** board. 2021-03-22 18:07:50 (UTC+0)

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

Grunny added a comment. 2021-03-22 18:38:09 (UTC+0)

> In ~~**T278014#6935675**~~, **@sbassett** wrote:
>
> > In ~~**T278014#6935629**~~, **@Grunny** wrote:
> > *Thanks, @sbassett ! Just for my reference on if I find any more of these in core or WMF deployed extensions, is it OK to push straight to Gerrit, and I assume we'd still want a ticket created for reference?*
>
> *I would say likely, yes. However it's probably a good idea to continue filing these as private bugs so the Security-Team can review them (our weekly clinic meeting is Monday morning) just to verify they are indeed low-risk and to also time them well for the weekly train deployment, in getting pushed to gerrit.*

Sounds good, thanks!

Reedy added a parent task: ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-03-30 00:46:14 (UTC+0)

Reedy closed this task as *Resolved*. 2021-03-30 00:48:34 (UTC+0)

Reedy assigned this task to **Grunny**.

Reedy mentioned this in ~~**T270459: Tracking bug for MediaWiki 1.31.13/1.35.2**~~. 2021-04-04 21:29:35 (UTC+0)

gerritbot added a comment. 2021-04-04 21:37:20 (UTC+0)

Change 676795 had a related patch set uploaded (by Reedy; author: Grunny):

[mediawiki/core@REL1_31] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/676795

gerritbot added a project: **Patch-For-Review**. 2021-04-04 21:37:21 (UTC+0)

gerritbot added a comment. 2021-04-04 21:44:01 (UTC+0)

Change 676795 **merged** by jenkins-bot:

[mediawiki/core@REL1_31] Escape mediastatistics-header-* messages on Special:NewFiles

https://gerrit.wikimedia.org/r/676795

Reedy added a project: ~~**MW-1.31-release**~~. 2021-04-04 21:45:09 (UTC+0)

ReleaseTaggerBot added a project: ~~**MW-1.31-release-notes**~~. 2021-04-04 22:00:19 (UTC+0)

Maintenance_bot removed a project: **Patch-For-Review**. 2021-04-04 22:10:17 (UTC+0)

Reedy renamed this task from *Unescaped messages used in HTML on Special:NewFiles* to *CVE-2021-30154: Unescaped messages used in HTML on Special:NewFiles*. 2021-04-06 19:11:24 (UTC+0)

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