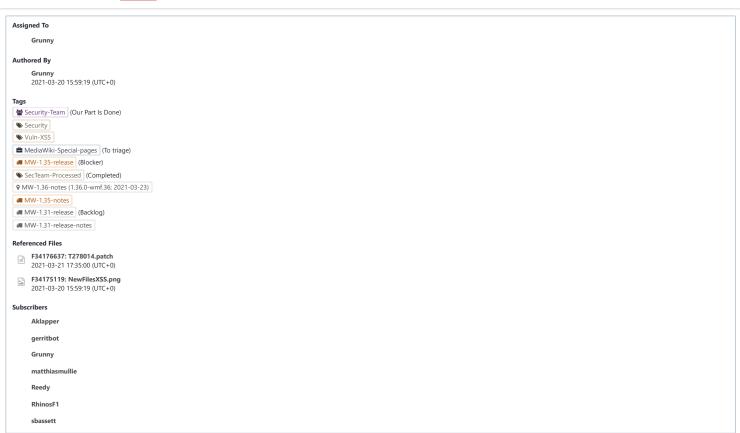
🕏 Maniphest 🧦 T278014

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

☑ Closed, Resolved ☑ Public SECURITY

Actions



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

Steps to reproduce:

Description

1. Edit one of the mediastatistics-header-* messages (e.g. edit MediaWiki:Mediastatistics-header-drawing) and add a simple XSS string like

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**





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 (1.36.8-wnnf.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 #278014#6935629, @Grunny wrote: Thanks, @sbassett Just for my reference on if find any more of these in core or WMF deployed extensions, is it OK to push straight to Gerrit, and 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 the weekly train deployment, in getting pushed to gerrit.	nem
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.	-
In #278014#6935629, @Srunny wrote: Thanks, @sbassett Just for my reference on if 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!	1
% 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 <i>Resolved.</i> 2021-03-30 00:48:34 (UTC+0)	
Reedy assigned this task to Grunny. On Productive of this is a record of the control of the co	
% Reedy mentioned this in 1270439. Tracking bug for MediaWiki 1.31.13/1.35.2. 2021-04-04 21:29:35 (UTC+0)	-
p gerritbot added a comment. 2021-04-04 21:37:20 (UTC+0)	1.
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: WW+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)	