

✓ XSS in Extension:RSS when \$wgRSSAllowLinkTag = true (CVE-2022-29969)

Actions

✓ Closed, Resolved

Public

SECURITY

Assigned To

Bawolff

Authored By

Bawolff

2022-04-27 17:45:27 (UTC+0)

Tags

Security-Team (Incoming)

Security

MediaWiki-extensions-RSS (Backlog)

Patch-For-Review

MW-1.39-notes (1.39.0-wmf.10; 2022-05-02)

Referenced Files

F35071953: T307028.patch
2022-04-28 12:06:36 (UTC+0)

Subscribers

Aklapper

Bawolff

gerritbot

Legoktm

sbassett

Description

CVE-2022-29969

This is a WMF deployed extension, however \$wgRSSAllowLinkTag is false on cluster, so it is not vulnerable in the configuration used by WMF.

RSS extension implementation of strip markers suffers from a similar problem as MW core's used to before **T110143** was fixed. When \$wgRSSAllowLinkTag is set to true, you can use this to escape from an attribute.

As an example:

- Set \$wgRSSAllowLinkTag = true;

Create an rss feed as follows:

```
<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
>

<channel>
  <title>Test</title>
  <item>
    <title>First item</title>
    <link>https://example.com</link>
    <description><![CDATA[<a title="tabindex=1 autofocus
onmouseover=alert(1) onfocus=blur() onblur=alert(document.domain)//"> Should autotrigger on chrome,
and trigger on hover on firefox</a> ]]></description>
  </item>
</channel>
</rss>
```

- Be sure the above RSS feed is added to \$wgRSSUrlWhitelist
- Create a template named Template:RSS containing only

```
<div title="{{description}}"></div>
```

- Use the following tag on a page <rss
templatename=RSS>http://address.of.rss.feed.from.above</rss>





This should make an XSS that autotriggers on chrome, and triggers on hoover in firefox.

Best solution, is to probably copy what MW core does for strip markers with them including ' '

Details

Risk Rating
Low

Author Affiliation
Wikimedia Communities

Project	Subject
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute
 mediawiki/extensions/RSS	SECURITY: Prevent XSS from "stripltem" replacement strings in attribute

[Customize query in gerrit](#)

Related Objects

Mentions

Mentioned In


~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~

Mentioned Here

~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~

[T203210: Extension:RSS shouldn't invent its own way to escape and parse things](#)

~~T110143: strip markers can be used to get around html attribute escaping in (many?) parser tags~~

 **Bawolff** created this task. 2022-04-27 17:45:27 (UTC+0)

  Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2022-04-27 17:45:28 (UTC+0)

 **Bawolff** added a project: **MediaWiki-extensions-RSS**. 2022-04-27 17:46:38 (UTC+0)

 **Legoktm** added a subscriber: **Legoktm**. 2022-04-27 17:57:27 (UTC+0) 

Is this related to **T203210: Extension:RSS shouldn't invent its own way to escape and parse things**?

 **Bawolff** added a comment. Edited · 2022-04-27 18:39:35 (UTC+0) 

Its related to the custom strip marker scheme, i'm not sure if that's what is being referred to in the other task. The code path involved here is the one using the Sanitizer, not the one with a custom escaping function.

The actual escapeTemplateParameter isn't really a security boundry most of the time except when used with insertStripItem, since the results get parsed later in most cases.

 **Bawolff** added a comment. 2022-04-28 12:06:36 (UTC+0) 

Proposed patch



T307028.patch 1 KB

Download

Extension doesn't seem to have a maintainer to CC on this task. I assume I should not just throw on gerrit since its WMF deployed, even if this code path is not enabled on cluster.

 **Bawolff** added a project: **Patch-For-Review**. 2022-04-28 12:22:37 (UTC+0)

 **sbassett** mentioned this in ~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~. 2022-04-28 21:23:09 (UTC+0)

 **sbassett** added a subscriber: **sbassett**. Edited · 2022-04-28 21:33:41 (UTC+0) 

In ~~T307028#7887638~~, @Bawolff wrote:

Extension doesn't seem to have a maintainer to CC on this task. I assume I should not just throw on gerrit since its WMF deployed, even if this code path is not enabled on cluster.

Since ext:RSS [isn't bundled](#), it would go out with the next supplemental release, which is tracked at **T305209**. I've added it there for now. Since this isn't currently vulnerable within Wikimedia production (and likely wouldn't ever be) I'd consider it low risk pushing it through gerrit. I think the only concern would be if other mediawiki operators were left uninformed or vulnerable for some time period, but IME we've tended not to care about that as much in the past and have just tried to merge security bug fixes quickly, make tasks public and send out the supplemental release each quarter, as best efforts.

 **Bawolff** added a comment. 2022-04-29 19:10:04 (UTC+0) 

<https://gerrit.wikimedia.org/r/c/mediawiki/extensions/RSS/+/787807> . I guess i shouldn't +2 myself, so if anyone wants to review...

 **Legoktm** added a subscriber: **gerritbot**. 2022-04-29 21:18:38 (UTC+0)

 **gerritbot** added a comment. 2022-04-29 21:20:46 (UTC+0) 

Change 787807 **merged** by jenkins-bot:

[mediawiki/extensions/RSS@master] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787807>

 **Bawolff** closed this task as *Resolved*. 2022-04-29 21:21:55 (UTC+0)

 **Bawolff** claimed this task.

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

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

 **gerritbot** added a comment. 2022-04-29 21:22:44 (UTC+0) 

Change 787779 had a related patch set uploaded (by Legoktm; author: Brian Wolff):

[mediawiki/extensions/RSS@REL1_38] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787779>

 **gerritbot** added a comment. 2022-04-29 21:23:03 (UTC+0) 

Change 787780 had a related patch set uploaded (by Legoktm; author: Brian Wolff):

[mediawiki/extensions/RSS@REL1_37] SECURITY: Prevent XSS from "striptem" replacement strings in attribute


<https://gerrit.wikimedia.org/r/787780>

 **gerritbot** added a comment. 2022-04-29 21:23:28 (UTC+0) 

Change 787781 had a related patch set uploaded (by Legoktm; author: Brian Wolff):

[mediawiki/extensions/RSS@REL1_36] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787781>

 **gerritbot** added a comment. 2022-04-29 21:23:43 (UTC+0) 

Change 787782 had a related patch set uploaded (by Legoktm; author: Brian Wolff):

[mediawiki/extensions/RSS@REL1_35] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787782>

 **gerritbot** added a comment. 2022-04-29 21:23:44 (UTC+0) 

Change 787783 had a related patch set uploaded (by Brian Wolff; author: Brian Wolff):

[mediawiki/extensions/RSS@REL1_34] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787783>

 **gerritbot** added a comment. 2022-04-29 21:24:29 (UTC+0) 

Change 787779 **merged** by jenkins-bot:

[mediawiki/extensions/RSS@REL1_38] SECURITY: Prevent XSS from "striptem" replacement strings in attribute



<https://gerrit.wikimedia.org/r/787779>

 **gerritbot** added a comment. 2022-04-29 21:26:05 (UTC+0) 

Change 787780 **merged** by jenkins-bot:

[mediawiki/extensions/RSS@REL1_37] SECURITY: Prevent XSS from "striptem" replacement strings in attribute



<https://gerrit.wikimedia.org/r/787780>

 **gerritbot** added a comment. 2022-04-29 21:26:58 (UTC+0) 

Change 787781 **merged** by jenkins-bot:

[mediawiki/extensions/RSS@REL1_36] SECURITY: Prevent XSS from "striptem" replacement strings in attribute



<https://gerrit.wikimedia.org/r/787781>

 **gerritbot** added a comment. 2022-04-29 21:27:25 (UTC+0) 

Change 787783 **merged** by Brian Wolff:

[mediawiki/extensions/RSS@REL1_34] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787783>

 **gerritbot** added a comment. 2022-04-29 21:27:32 (UTC+0) 


Change 787782 **merged** by jenkins-bot:

[mediawiki/extensions/RSS@REL1_35] SECURITY: Prevent XSS from "striptem" replacement strings in attribute

<https://gerrit.wikimedia.org/r/787782>

 **ReleaseTaggerBot** added a project: ~~MW-1.39-notes (1.39.0-wmf.10; 2022-05-02)~~. 2022-04-29 22:00:36 (UTC+0)

 **Bawolff** updated the task description. (**Show Details**) 2022-08-16 08:09:54 (UTC+0)

 **sbassett** renamed this task from *XSS in Extension:RSS when \$wgRSSAllowLinkTag = true;* to *XSS in Extension:RSS when \$wgRSSAllowLinkTag = true (CVE-2022-29969)*. 2022-08-16 13:36:57 (UTC+0)

→ **sbassett** triaged this task as *Low* priority.

 **sbassett** changed Risk Rating from N/A to Low.