

📌 Invoking any namespaced page with {{#widget:}} will run the page's contents as a widget; even if the page is not in Widget namespace (CVE-2020-9382)

☑ Closed, ResolvedPublicSECURITY

≡Actions

Assigned To

Alexia

Authored By

Alexia
2020-02-21 17:40:48 (UTC+0)

Tags

🔒 Security

📁 MediaWiki-General

📁 MediaWiki-extensions-Widgets (Backlog)

Referenced Files

None

Subscribers

Aklapper

Alexia

Bawolff

DannyS712

Ernstkm

Kghbln

Liuxinyu970226

View All 11 Subscribers

Description

Author Affiliation: Fandom(Wikia, Gamepedia)

This issue occurs since user input is passed to a function not safe for user input.

<https:// Gerrit Wikimedia.org/r/#/c/mediawiki/extensions/Widgets/+/-/574041/>

<https:// Gitlab.com/hydrawiki/third-party-extensions/issues/103>

The {{#widget:}} tag can invoke non-widget pages (aside from mainspace pages) by simply invoking the full page name with the widget tag e.g. {{#widget:Template:Page name}}, which can allow any user to run style and script tags on any page.
Example provided by Dragalia Lost admins:

<https://dragalialost.gamepedia.com/Test2>

<https://dragalialost.gamepedia.com/Template:Test2/css>

Details

Author Affiliation

Other (Please specify in description)

Related Objects

Q Search... ▾

Task Graph	Mentions	
Status	Assigned	Task
☑ Resolved	Reedy	T240392 Release MediaWiki 1.31.7/1.33.3/1.34.1
🔒 ☑ Resolved	sbassett	T240400 Write and send supplementary release announcement for extensions and skins with security patches (MediaWiki 1.31.7/1.33.3/1.34.1)
☑ Resolved	Alexia	T245050 Invoking any namespaced page with {{#widget:}} will run the page's contents as a widget; even if the page is not in Widget namespace (CVE-2020-9382)

- 🔧 Alexia created this task. 2020-02-21 17:40:48 (UTC+0)
- 👤 🛡 Restricted Application added a subscriber: Aklapper. · View Herald Transcript 2020-02-21 17:40:50 (UTC+0)
- 🔗 Aklapper added a project: MediaWiki-General. 2020-02-21 23:16:33 (UTC+0)
- ➡ • chasemp triaged this task as Medium priority. 2020-02-24 16:09:53 (UTC+0)
- ☑ Alexia closed this task as Resolved. 2020-02-24 16:13:46 (UTC+0)
- 👤 Alexia claimed this task.
- This has been merged.
- <https://github.com/wikimedia/mediawiki-extensions-Widgets/blob/master/WidgetRenderer.php#L162>
- 🔔 sbassett reopened this task as Open. 2020-02-24 16:18:03 (UTC+0)
- 👤 sbassett removed Alexia as the assignee of this task.
- 🔗 sbassett edited projects, added MediaWiki-extensions-Widgets; removed Security-Team.
- 👤 sbassett added subscribers: siebrand, Reedy.

☒ **sbassett** closed this task as *Resolved*. Edited · 2020-02-24 16:26:13 (UTC+0)

 sbassett assigned this task to **Alexia**.

 sbassett added a subscriber: sbassett.

Whoops, I think this task was being edited as the [Security-Team](#) was reviewing it :) Did the above commit get deployed to any relevant wikis (I know ext:Widget isn't part of WMF production)? That should probably happen soon since the patch for master is public. We should also try to backport this to [supported release branches](#).

 Alexia added a comment. 2020-02-24 16:28:27 (UTC+0)

In [T245850#5912492](#), @sbassett wrote:

Whoops, I think this task was being edited as the **Security-Team** was reviewing it :) Did the above commit get deployed to any relevant wikis (I know ext:Widget isn't part of WMF production)? That should probably happen soon since the patch for master is public. We should also try to backport this to [supported release branches](#).

Yes, this patch is out to all gamepedia.com, wikia.org, and fandom.com wikis. I looked over WMF wikis and as far as I can tell WMF does not use Widgets.

 sbassett changed the visibility from "Custom Policy" to "Public (No Login Required)". 2020-02-24 20:54:44 (UTC+0)

 Restricted Application added a subscriber: **Liuxinyu970226**. · [View Herald Transcript](#) 2020-02-24 20:54:45 (UTC+0)

sbassett added a comment. 2020-02-24 21:01:45 (UTC+0)


Backports:

- <https://gerrit.wikimedia.org/r/574556> (REL1_31)
- <https://gerrit.wikimedia.org/r/574557> (REL1_33)
- <https://gerrit.wikimedia.org/r/574558> (REL1_34)

Also added to **T240400** for tracking and will request a CVE.

sbassett mentioned this in [T240400](#). Write and send supplementary release announcement for extensions and skins with security patches (MediaWiki 1.34.7/1.33.3/1.34.1). 2020-02-24 21:03:53 (UTC+0)

 Alexia updated the task description. (Show Details) 2020-02-24 21:24:20 (UTC+0)

 sbasnett renamed this task from *Invoking any namespaced page with `{{#widget:}}` will run the page's contents as a widget; even if the page is not in Widget namespace.* to *Invoking any namespaced page with `{{#widget:}}` will run the page's contents as a widget; even if the page is not in Widget namespace (CVE-2020-9382).* 2020-02-24 22:19:18 (UTC+0)

 Bawolff added a subscriber: **Bawolff**. 2020-02-25 00:00:32 (UTC+0)

The `{{#widget:}}` tag can invoke non-widget pages (aside from mainspace pages) by simply invoking the full page name with the widget tag e.g. `{{#widget:Template:Page name}}`, which can allow any user to run style and script tags on any page.

Just as a point of note, you can do mainspace pages by doubling the colon.

 Bawolff added a comment. 2020-02-25 00:03:34 (UTC+0)

This is a super commonly used extension in third party wikis. I think an email to mediawiki-l encouraging people to update might be a good idea.

 Kghbln added a subscriber: **Kghbln**. 2020-02-25 10:12:19 (UTC+0)

Since this is a versioned extension [@Yaron_Koren](#) may additionally want to release and tag a new version to make the need to upgrade visible even more.

 sbassett added a comment. 2020-02-25 16:28:55 (UTC+0)

In ~~T245850#5914122~~, @Bawolff wrote:

This is a super commonly used extension in third party wikis. I think an email to mediawiki-l encouraging people to update might be a good idea.

So we've tried to be a little better about this sort of information dispersal by adding tasks like **T240400** to the release process, the end result being quarterly-ish emails to relevant mailing lists (1, 2, etc). We can certainly send out something to that effect sooner (like today or tomorrow), focused on this specific issue, if you feel that is warranted.

sbassett added a parent task: ~~T240400: Write and send supplementary release announcement for extensions and skins with security patches (MediaWiki 1.31.7/1.33.3/1.34.1)~~. 2020-03-10 14:15:28 (UTC+0)

 DannyS712 added a subscriber: **DannyS712**. 2020-03-26 17:51:27 (UTC+0)

 Ernstkm added a subscriber: **Ernstkm**. 2020-05-26 22:55:14 (UTC+0)

Skizzerz mentioned this in ~~T269710: RCE in Widgets extension (CVE-2020-35625)~~. 2020-12-11 18:07:58 (UTC+0)