th Maniphest → T245850 Create Task

Actions

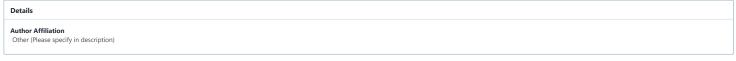
✓ Invoking any namespaced page with {{#widget:}} will run the page's contents as a widget; even if the page is not in Widget namespace (CVE-2020-9382)





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

View All 11 Subscribers





- 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)

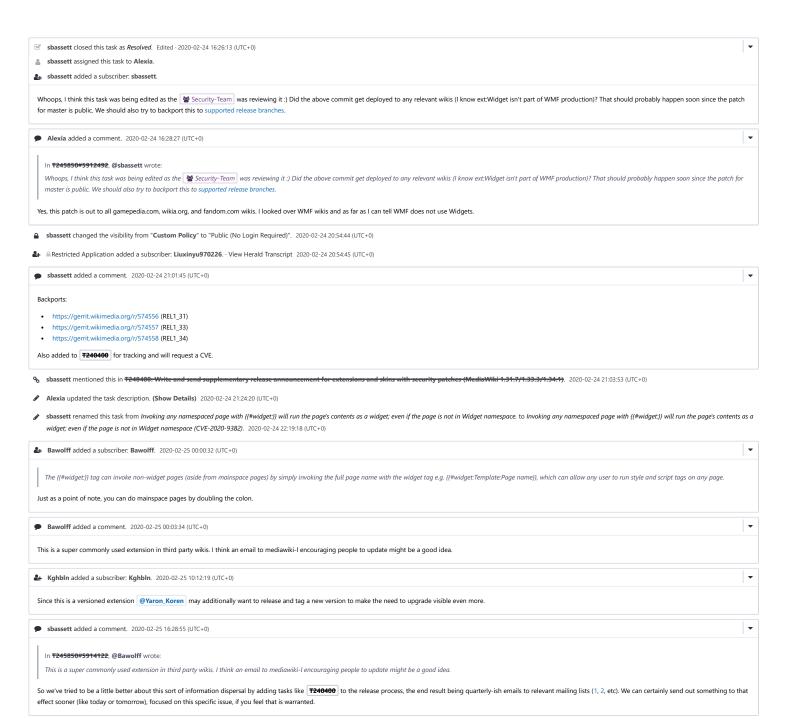
Alexia closed this task as Resolved. 2020-02-24 16:13:46 (UTC+0)

Alexia claimed this task.

This has been merged.

https://github.com/wikimedia/mediawiki-extensions-Widgets/blob/master/WidgetRenderer.php#L162

- **③ 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 added a parent task: #240400. Write and send supplementary release amnouncement for extensions and skins with security patches (MediaWiki 1.31.77/1.33.3/1.34.1). 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)