

✓ PollINy: Stored XSS (CVE-2020-29003)

✓ Closed, Resolved

🌐 Public

SECURITY

≡ Actions

Assigned To

ashley

Authored By

ashley
2020-10-26 20:43:57 (UTC+0)

Tags

🔒 Security

🔒 Vuln-XSS

📁 PollINy (Backlog)

🔗 Social-Tools (PollINy)

Referenced Files

F32416835: new-stored-xss-patch.patch
2020-10-27 21:19:33 (UTC+0)

F32415006: PollINy-Stored-XSS-T266508.patch
2020-10-26 20:48:48 (UTC+0)

Subscribers

Aklapper

ashley

Bawolff

Isarra

Icawte

Legoktm

sbassett

Description

Like **T266400** but only for **PollINy** this time around...

Prerequisites: [social tools](#) setup (MW 1.34 with [SocialProfile](#), and for this particular bug, also need [PollINy](#))

- Create a poll via `Special:CreatePoll`, or edit an existing one via `Special:UpdatePoll`
- Have an answer option contain something like `<script>alert('XSS')</script>`
- Save changes
- When viewing the poll's page in the `NS_POLL` namespace, the malicious code gets executed despite that it damn well shouldn't

The last step is also true for polls embedded on other wiki pages via the `pollembed` parser tag.

Details

Project	Subject
mediawiki/extensions/PollINy	[SECURITY] Fix stored XSS via poll choices on Poll: pages etc.
mediawiki/extensions/PollINy	[SECURITY] Fix stored XSS via poll choices on Poll: pages etc.

Customize query in [gerrit](#)

Related Objects

Mentions

Mentioned In

[T262810: Write and send supplementary release announcement for extensions and skins with security patches \(1.31.11/1.35.4\)](#)

Mentioned Here

[T248390: Better NoJS support](#)
[T266400: RandomGameUnit: Stored XSS \(CVE-2020-27957\)](#)

ashley created this task. 2020-10-26 20:43:57 (UTC+0)

Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2020-10-26 20:43:58 (UTC+0)


ashley claimed this task. 2020-10-26 20:44:26 (UTC+0)

ashley added projects: **Vuln-XSS**, **PollINy**.

Restricted Application added a project: **Social-Tools**. · View Herald Transcript 2020-10-26 20:44:27 (UTC+0)

ashley updated the task description. (**Show Details**) 2020-10-26 20:45:54 (UTC+0)

ashley moved this task from **Backlog** to **PollINy** on the **Social-Tools** board. 2020-10-26 20:48:01 (UTC+0)

 **PollNY-Stored-XSS-T266508.patch** 7 KB
Download

Proposed patch which fixes the issues noted here and includes some unrelated no-JS work ([T248390](#)); the relevant chunks are obviously the ones where `htmlspecialchars` is mentioned, except for the last one ("next poll" URL stuff), that's strictly no-JS related and not related to this ticket.

 **Legoktm** added a subscriber: **Legoktm**. 2020-10-27 17:06:03 (UTC+0)


```
@@ -230,8 +230,9 @@ class PollNYHooks {
    foreach ( $poll_info['choices'] as $choice ) {
        $output .= "<div class=\"poll-choice\">
-        <input type=\"radio\" name=\"poll_choice\" data-poll-id=\"{$poll_info['id']}\" data-poll-page-id=\"{$poll_page_id}\" id=\"poll_choice\" value=\"{$choice['id']}\">
+        <input type=\"radio\" name=\"poll_choice\" data-poll-id=\"{$poll_info['id']}\" data-poll-page-id=\"{$poll_page_id}\" id=\"poll_choice\" value=\"{$choice['id']}\">";
        $choice['choice']]
-        </div>;
+        <input type=\"radio\" name=\"poll_choice\" data-poll-id=\"{$poll_info['id']}\" data-poll-page-id=\"{$poll_page_id}\" id=\"poll_choice\" value=\"{$choice['id']}\">";
+        $output .= htmlspecialchars( $choice['choice'], ENT_QUOTES );
+        $output .= '</div>';
    }


    $output .= Html::submitButton( wfMessage( 'poll-submit-btn' )->escaped(), [ 'class' => 'poll-vote-btn-nojs' ] );
```

Do you want to apply the same `(int)` casting for these ids just to make it obvious these are safe? Or switch to the Html wrapper which should escape attributes I believe?

Other stuff LGTM.

 **sbassett** mentioned this in ~~[T263040-Write and send supplementary release announcement for extensions and skins with security patches \(1.31.14/1.35.4\)](#)~~. 2020-10-27 20:16:35 (UTC+0)

 **ashley** added a comment. 2020-10-27 21:19:33 (UTC+0)

 **new-stored-xss-patch.patch** 8 KB
Download

[@Legoktm](#) Thanks for the CR! While attempting to implement your changes, I found a few more nasty stored XSS lines in that same file...here's a new patch which hopefully catches 'em all, for good this time around.


 **Reedy** removed a project: **Security-Team**. 2020-11-02 16:03:41 (UTC+0)

 **ashley** added a subscriber: **Bawolff**. 2020-11-05 08:30:06 (UTC+0)

cc'ing [@Bawolff](#) for thoughts

 **Bawolff** added a comment. 2020-11-05 08:48:42 (UTC+0)

This looks like it fixes the XSS's properly, as far as that patch goes (I did not look at any of the other PollNY code beyond what was in the patch)

 **sbassett** added a subscriber: **sbassett**. 2020-11-05 20:33:05 (UTC+0)


+1 to the patch at [T266508#6583137](#). One thing I did notice was that in `PollNY.hooks.php`, the `$choice['percent']` variable used to build the html string on [line 263](#) isn't cast to an `int` as similar variables are within the patch. The cast likely isn't necessary, even though this does appear to be a database value as opposed to a computed value as the similar percent variables are within `PollPage.class.php`. Just pointing out for consistency's sake.

 **Legoktm** closed this task as *Resolved*. 2020-11-16 18:35:36 (UTC+0)

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

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

 **sbassett** renamed this task from *PollNY: Stored XSS* to *PollNY: Stored XSS (CVE-2020-29003)*. 2020-12-01 17:47:20 (UTC+0)

 **gerritbot** added a comment. 2020-12-22 21:20:39 (UTC+0)

Change 651588 had a related patch set uploaded (by SBassett; owner: Jack Phoenix):
[mediawiki/extensions/PollNY@REL1_35] [SECURITY] Fix stored XSS via poll choices on Poll: pages etc.

<https://gerrit.wikimedia.org/r/651588>

 **gerritbot** added a project: **Patch-For-Review**. 2020-12-22 21:20:40 (UTC+0)

 **gerritbot** added a comment. 2020-12-22 21:31:35 (UTC+0)

Change 651588 **merged** by jenkins-bot:
[mediawiki/extensions/PollNY@REL1_35] [SECURITY] Fix stored XSS via poll choices on Poll: pages etc.

<https://gerrit.wikimedia.org/r/651588>

 **Maintenance_bot** removed a project: **Patch-For-Review**. 2020-12-22 22:10:28 (UTC+0)