

CVE-2021-30152: action=protect lets users with 'protect' permission protect to higher protection level

✓ Closed, Resolved

🌐 Public

SECURITY

≡ Actions

Assigned To

Reedy

Authored By

Tobi_406

2020-12-22 16:53:49 (UTC+0)

Tags

📁 MediaWiki-Action-API (Unsorted)

🔒 Security

👤 Security-Team (Our Part Is Done)

🔒 Vuln-MissingAuthz (Tracked)

🔧 Patch-For-Review

👤 Platform Team Workboards (Clinic Duty Team) (Later)

👤 MW-1.37-notes (1.37.0-wmf.1; 2021-04-13)

📁 MW-1.36-notes (Backlog)

Referenced Files

📄

F33984659: T270713-master.patch

2021-01-04 18:08:54 (UTC+0)

📄

F33984579: Screenshot 2021-01-04 at 17.13.56.png

2021-01-04 17:14:21 (UTC+0)

📄

F33984567: Screenshot 2021-01-04 at 17.05.20.png

2021-01-04 17:07:04 (UTC+0)

📄

F33984569: Screenshot 2021-01-04 at 17.06.16.png

2021-01-04 17:07:04 (UTC+0)

📄

F33984557: Screenshot 2021-01-04 at 16.58.40.png

2021-01-04 17:03:19 (UTC+0)

Subscribers

Aklapper

daniel

DannyS712

gerritbot

Legoktm

Magiczocker10

MarkusRost


[View All 10 Subscribers](#)

Description

If a user with `protect` permission protects a page using APISandbox they can protect the page to a higher protection level than they can edit. If `action=edit` and `action=protect` are not restricted, the user can also unprotect the page

How to reproduce

- Add the following to `LocalSettings.php`:

```
$wgGroupPermissions['protect']['protect'] = true;
```
- Create an account and assign it to the `protect` group (for example, using maintenance scripts, `php maintenance/createAndPromote.php --custom-groups protect TestUser TestPassword`)
- Login as the newly created user
- Go to `index.php?title=TestPage&action=protect`
 - see that user can't protect to "allow only administrators"
- 
- Go to `index.php?title=Special:APISandbox#action=protect&format=json&title=TestPage&protections=create%3Dsyp`
 - you can also choose other protection levels and types from `$wgRestrictionLevels` and `$wgRestrictionTypes` respectively
 - click `action=protect`
 - hit "auto-fill the token"
 - hit "make request"

```
Request URL:
{
  "protect": {
    "title": "TestPage",
    "reason": "",
    "protections": [
      {
        "create": "sysop",
        "expiry": "infinite"
      }
    ]
  }
}

Request time: 195 ms
```

- Go to `index.php?title=TestPage&action=history`
- see that page is protected so that only administrators may create it

Information for "TestPage"

Basic information

History title	TestPage
Default view key	TestPage
Page length in bytes	0
Page ID	0
Page content language	en-gb: British English
Page content model	external changes
Indexing by robots	Disallowed
Number of redirects to this page	0
Number of subpages of this page	0 (0 redirects, 0 non-redirects)
Page views in the past 30 days	0

Page protection

Create: allow only administrators (initial)

View the protection log for this page

- You can also remove the protection level again by going to `Special:ApiSandbox#action=protect&format=json&title=TestPage&protections=create%3Dall`
- this doesn't work if you've previously restricted the `edit` and/or `protect` types

```
Request URL:
{
  "protect": {
    "title": "TestPage",
    "reason": "",
    "protections": [
      {
        "create": "",
        "expiry": "infinite"
      }
    ]
  }
}

Request time: 60 ms
```

(Credit for finding this goes to my friend Magiczocker10)

Details

Project	Subject
mediawiki/core	SECURITY: Allow user to only apply protection they have right to do so via action=protect
mediawiki/core	SECURITY: Allow user to only apply protection they have right to do so via action=protect
mediawiki/core	SECURITY: Allow user to only apply protection they have right to do so via action=protect
mediawiki/core	SECURITY: Allow user to only apply protection they have right to do so via action=protect

[Customize query in Gerrit](#)

Related Objects

Q Search...

Task Graph	Mentions	
Status	Assigned	Task
<div><div><div></div></div><div>Resolved</div></div>	Reedy	<div><div><div><div></div></div><div><div>T270458</div></div></div>Release MediaWiki 1.31.13/1.35.2</div>
<div><div><div></div></div><div>Resolved</div></div>	Reedy	<div><div><div><div></div></div><div><div>T270459</div></div></div>Tracking bug for MediaWiki 1.31.13/1.35.2</div>
<div><div><div></div></div><div>Resolved</div></div>	Reedy	<div><div><div><div></div></div><div><div>T270713</div></div></div>CVE-2021-30152: action=protect lets users with 'protect' permission protect to higher protection level</div>

- 🔧 [Tobi_406](#) created this task. 2020-12-22 16:53:49 (UTC+0)
- 👤 [Restricted Application](#) added a subscriber: [Aklapper](#). · View Herald Transcript 2020-12-22 16:53:49 (UTC+0)
- 🔧 [Tobi_406](#) renamed this task from *APISandbox lets users with 'protect' permission bypass protection levels* to *APISandbox lets users with 'protect' permission protect to higher protection level*. 2020-12-22 16:54:08 (UTC+0)
- 🔧 [Tobi_406](#) updated the task description. ([Show Details](#)) 2020-12-22 18:32:40 (UTC+0)
- 🔧 [Legoktm](#) set Security to Software security bug. 2020-12-22 18:33:40 (UTC+0)
- 🔗 [Legoktm](#) added projects: [Security](#), [Security-Team](#).
- 🔒 [Legoktm](#) changed the visibility from "Public (No Login Required)" to "[Custom Policy](#)".
- 🔧 [Legoktm](#) changed the subtype of this task from "Task" to "Security Issue".
- 👤 [Legoktm](#) added a subscriber: [Legoktm](#).
- 🔧 [Tobi_406](#) updated the task description. ([Show Details](#)) 2020-12-22 18:59:10 (UTC+0)
- 👤 [Tobi_406](#) added subscribers: [Magiczocker10](#), [MarkusRost](#).

👤 [DannyS712](#) added a subscriber: [DannyS712](#). 2020-12-22 23:53:30 (UTC+0)


[@Tobi_406](#) are you sure this is due to the api sandbox and not the api itself? The api should just be calling the relevant action specified and not override any of the behavior

💬 [Tobi_406](#) added a comment. 2020-12-23 00:04:54 (UTC+0)

The api should just be calling the relevant action specified and not override any of the behavior

Do you mean the api samdbox in that sentence?
But no, I'm not sure, I wasn't able to get it working to check with the API directly (I don't use it often, sorry).

So I used ApiSandbox and to make the task as detailed as possible I specified I used ApiSandbox.
But yes, I do think it has to do with the API, just don't have any evidence for that.

 **Danny5712** added a comment. 2020-12-23 00:10:42 (UTC+0)

In **T270713#6709472**, @Tobi_406 wrote:

The api should just be calling the relevant action specified and not override any of the behavior


Do you mean the api sandbox in that sentence?


But no, I'm not sure, I wasn't able to get it working to check with the API directly (I don't use it often, sorry).

So I used ApiSandbox and to make the task as detailed as possible I specified I used ApiSandbox.


But yes, I do think it has to do with the API, just don't have any evidence for that.

Yes, sorry, I meant "the api sandbox should just be calling the relevant action specified and not override any of the behavior"

 **Reedy** added a project: **Vuln-MissingAuthz**. 2020-12-23 03:33:19 (UTC+0)

 **sbasset** moved this task from **Incoming** to **Watching** on the **Security-Team** board. 2021-01-04 16:10:26 (UTC+0)

 **Reedy** updated the task description. (**Show Details**) 2021-01-04 17:03:19 (UTC+0)

 **Reedy** added a subscriber: **Reedy**.


<https://www.mediawiki.org/w/api.php?action=help&modules=protect>
<https://www.mediawiki.org/w/api.php?action=paraminfo&modules=protect>

 **Reedy** updated the task description. (**Show Details**) 2021-01-04 17:07:04 (UTC+0)

 **Reedy** added a project: **Platform Engineering**. 2021-01-04 17:10:42 (UTC+0)

I will note that allowing users to protect higher than their rights allow isn't necessarily an issue. Being able to remove that is more of an issue.
And there's the discrepancy between endpoints

 **Reedy** updated the task description. (**Show Details**) 2021-01-04 17:12:43 (UTC+0)

 **Reedy** updated the task description. (**Show Details**)

 **Reedy** added a comment. Edited · 2021-01-04 17:34:44 (UTC+0)

The user facing form does

```
$levels = $this->permManager->getNamespaceRestrictionLevels(  
    $this->mTitle->getNamespace(), $this->mContext->getUser()  
);
```

and

```
$val = $request->getVal( "mwProtect-level-$action" );  
if ( isset( $val ) && in_array( $val, $levels ) ) {  
    $this->mRestrictions[$action] = $val;  
}
```

~~the API doesn't do anything with getNamespaceRestrictionLevels. No validation~~

We can't fix the API allowed parameters, to be documented in the autogenerated page, as it can vary between pages (or, well, Namespaces)

```
'protections' => [  
    ApiBase::PARAM_ISMULTI => true,  
    ApiBase::PARAM_REQUIRED => true,  
],
```

 **Reedy** added a comment. Edited · 2021-01-04 17:56:14 (UTC+0)

Ok, so looking further, the problem is the way the API does the validation;

```
if ( !in_array( $p[1], $this->getConfig()->get( 'RestrictionLevels' ) ) && $p[1] != 'all' ) {  
    $this->dieWithError( [ 'apierror-protect-invalidlevel', wfEscapeWikiText( $p[1] ) ] );  
}
```

It just uses effectively `$wgRestrictionLevels` which is not modified for the user

```
> var_dump( $wgRestrictionLevels );  
/var/www/wiki/mediawiki/core/maintenance/eval.php(82) : eval()'d code:1:  
array(3) {  
  [0] =>  
  string(0) ""  
  [1] =>  
  string(13) "autoconfirmed"  
  [2] =>  
  string(5) "sysop"  
}
```

The error message is

```
"apierror-protect-invalidlevel": "Invalid protection level \"${1}\".",
```

 **Reedy** added a comment. 2021-01-04 18:02:10 (UTC+0)

So for a patch that should be good for production.. As yet untested..

```
diff --git a/includes/api/ApiProtect.php b/includes/api/ApiProtect.php  
index 16f7a55a56..50f2521caf 100644  
--- a/includes/api/ApiProtect.php  
+++ b/includes/api/ApiProtect.php
```

```
@@ -67,6 +67,10 @@ class ApiProtect extends ApiBase {
    }

    $restrictionTypes = $titleObj->getRestrictionTypes();
+    $levels = $this->getPermissionManager()->getNamespaceRestrictionLevels(
+        $titleObj->getNamespace(),
+        $user
+    );

    $protections = [];
    $expiryarray = [];
@@ -85,7 +89,7 @@ class ApiProtect extends ApiBase {
    if ( !in_array( $p[0], $restrictionTypes ) && $p[0] != 'create' ) {
        $this->dieWithError( [ 'apierror-protect-invalidaction', wfEscapeWikiText( $p[0] ) ] );
    }
-    if ( !in_array( $p[1], $this->getConfig()->get( 'RestrictionLevels' ) ) && $p[1] != 'all' ) {
+    if ( !in_array( $p[1], $levels ) && $p[1] != 'all' ) {
        $this->dieWithError( [ 'apierror-protect-invalidlevel', wfEscapeWikiText( $p[1] ) ] );
    }
}
```

It will give the "Invalid protection level" error, which technically isn't correct, but is better than just allowing it.

Also, adding i18n messages into WMF production in security patches is painful. So we won't do that

We can do a followup/add on patch for this to add another message to be used in this case. It depends whether we really care about differentiating between "invalid" restrictions, and restrictions that are "invalid" (or rather, not allowed) for that user

Which means a patch more like

```
diff --git a/includes/api/ApiProtect.php b/includes/api/ApiProtect.php
index 16f7a55a56..7abedede93 100644
--- a/includes/api/ApiProtect.php
+++ b/includes/api/ApiProtect.php
@@ -67,6 +67,10 @@ class ApiProtect extends ApiBase {
    }


    $restrictionTypes = $titleObj->getRestrictionTypes();
+    $levels = $this->getPermissionManager()->getNamespaceRestrictionLevels(
+        $titleObj->getNamespace(),
+        $user
+    );

    $protections = [];
    $expiryarray = [];
@@ -88,6 +92,10 @@ class ApiProtect extends ApiBase {
    if ( !in_array( $p[1], $this->getConfig()->get( 'RestrictionLevels' ) ) && $p[1] != 'all' ) {
        $this->dieWithError( [ 'apierror-protect-invalidlevel', wfEscapeWikiText( $p[1] ) ] );
    }
+    if ( !in_array( $p[1], $levels ) && $p[1] != 'all' ) {
+        // TODO: Add new message for "user isn't allowed to add this protection"
+        $this->dieWithError( [ 'apierror-protect-invalidlevel', wfEscapeWikiText( $p[1] ) ] );
+    }

    if ( wfIsInfinity( $expiry[1] ) ) {
        $expiryarray[ $p[0] ] = 'infinity';
    }
}
```

I don't imagine this is actually necessary, so we can probably just re-purpose this message for the master/deployment branch patches

Reedy added a comment. 2021-01-04 18:08:54 (UTC+0)

 **T270713-master.patch** 1 KB
Download

is basically the first first posted above; no i18n changes

Reedy added a project: **Patch-For-Review**. 2021-01-04 18:09:06 (UTC+0)

Reedy renamed this task from *APISandbox lets users with 'protect' permission protect to higher protection level* to *action=protect lets users with 'protect' permission protect to higher protection level*. 2021-01-04 18:11:59 (UTC+0)

Reedy added a parent task: ~~T270459~~ **Tracking bug for MediaWiki 1.31.13/1.35.2**.

MarkusRost added a comment. 2021-01-04 18:22:10 (UTC+0)

Wouldn't returning a permissions error be the better message? That message should already exist as well and the user is in fact missing the permission to protect to that level.

Reedy added a comment. 2021-01-04 18:33:31 (UTC+0)

If you can find a better pre-existing message, sure.

Like I say, I'm not adding (or altering an existing) message for the patch deployed to Wikimedia production. We can do so for a patch that eventually lands in master and release branches.

There's some similar, but not quite right messages, for example:

```
"protect-locked-access": "Your account does not have permission to change page protection levels.\nHere are the current settings for the page <strong>$1</strong>:",
```

It kinda looks like the form for protect just silently discards it where the user doesn't have the right, so some error from the API is better than the apparent silent failure

```
$val = $request->getVal( "mwProtect-level-$action" );
if ( isset( $val ) && in_array( $val, $levels ) ) {
    $this->mRestrictions[ $action ] = $val;
}
```

holger.knust triaged this task as *High* priority. 2021-01-05 21:19:00 (UTC+0)

holger.knust edited projects, added **Platform Team Workboards (Clinic Duty Team)**; removed **Platform Engineering**.

holger.knust moved this task from **Inbox** to **Later** on the **Platform Team Workboards (Clinic Duty Team)** board.



















sbasset added a subscriber: **sbasset**. 2021-01-14 19:22:11 (UTC+0)

sbasset moved this task from **Watching** to **Security Patch To Deploy** on the **Security-Team** board. 2021-01-27 21:49:06 (UTC+0)

Reedy added a comment. 2021-01-29 20:44:07 (UTC+0)

Should probably get this deployed...

sbasset moved this task from **Security Patch To Deploy** to **Our Part Is Done** on the **Security-Team** board. Edited · 2021-02-01 22:06:56 (UTC+0)

Deployed the patch from T270713#6720158 to wmf.27. Logs seem fine.	
 daniel added a subscriber: daniel . 2021-03-25 09:49:33 (UTC+0)	▼
What's the status here? Is this fixed in master?	
 sbassett added a comment. 2021-03-25 14:16:02 (UTC+0)	▼
In T270713#6944605 , @ daniel wrote: <i>What's the status here? Is this fixed in master?</i>	
The security patch is deployed per T270713#6794141 (also tracked at T276237) and being held for the next security release, which I'd imagine will be out in the next couple of weeks. So no, not on master yet. The tracking task for embargoed security bugs is here: T270459 .	
 Reedy mentioned this in T270459 - Tracking bug for MediaWiki 1.34-1.37/1.35-2 2021-03-30 00:40:05 (UTC+0)	
 Reedy claimed this task. 2021-03-30 01:07:51 (UTC+0)	
 Reedy closed this task as <i>Resolved</i> . 2021-04-04 22:33:43 (UTC+0)	▼
Master patch applies cleanly on 1.35 and 1.31. Wheee.	
 Reedy renamed this task from <i>action=protect lets users with 'protect' permission protect to higher protection level to [CVE-2021-30152] action=protect lets users with 'protect' permission protect to higher protection level</i> . 2021-04-06 19:09:25 (UTC+0)	
 Reedy renamed this task from <i>[CVE-2021-30152] action=protect lets users with 'protect' permission protect to higher protection level</i> to <i>CVE-2021-30152: action=protect lets users with 'protect' permission protect to higher protection level</i> .	
 Reedy added a subscriber: gerritbot . 2021-04-08 19:11:18 (UTC+0)	
 gerritbot added a comment. 2021-04-08 19:50:21 (UTC+0)	▼
Change 678032 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@REL1_31] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678032	
 gerritbot added a comment. 2021-04-08 19:53:00 (UTC+0)	▼
Change 678038 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@REL1_35] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678038	
 gerritbot added a comment. 2021-04-08 19:59:09 (UTC+0)	▼
Change 678032 merged by jenkins-bot: [mediawiki/core@REL1_31] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678032	
 gerritbot added a comment. 2021-04-08 20:14:31 (UTC+0)	▼
Change 678038 merged by jenkins-bot: [mediawiki/core@REL1_35] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678038	
 gerritbot added a comment. 2021-04-08 20:43:06 (UTC+0)	▼
Change 678073 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@master] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678073	
 Reedy changed the visibility from "Custom Policy" to "Public (No Login Required)". 2021-04-08 21:07:43 (UTC+0)	
 Reedy mentioned this in T279717: Followup to T270713 .	
 Bugreporter mentioned this in T27005: Fix wgRestrictionLevels for all Serbian projects to fully work 2021-04-08 21:43:27 (UTC+0)	
 gerritbot added a comment. 2021-04-08 22:12:31 (UTC+0)	▼
Change 678073 merged by jenkins-bot: [mediawiki/core@master] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/678073	
 gerritbot added a comment. 2021-04-08 22:16:43 (UTC+0)	▼
Change 677962 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@REL1_36] SECURITY: Allow user to only apply protection they have right to do so via action=protect https://gerrit.wikimedia.org/r/677962	

 ReleaseTaggerBot added a project: ~~MW-1.37-notes (1.37.0-wmf.1, 2021-04-13)~~. 2021-04-08 23:00:36 (UTC+0)

 geritbot added a comment. 2021-04-09 00:31:35 (UTC+0) 

Change 677962 **merged** by jenkins-bot:

[mediawiki/core@REL1_36] SECURITY: Allow user to only apply protection they have right to do so via action=protect

<https://gerrit.wikimedia.org/r/677962>

 ReleaseTaggerBot added a project: ~~MW-1.36-notes~~. 2021-04-09 01:00:36 (UTC+0)