

BlockLogFormatter can output raw html (CVE-2020-35478, CVE-2020-35479)

Closed, Resolved

Public

SECURITY

Actions

Assigned To

Umherirrender

Authored By

Umherirrender
2020-11-29 11:17:31 (UTC+0)

Tags

- Security-Team (Our Part Is Done)
- Security
- MediaWiki-Blocks (Backlog)
- MediaWiki-Logevents (Backlog)
- Anti-Harassment (The Letter Song) (Done: Q2 (2020-2021) ✓)
- MW-1.36-notes (1.36.0-wmf.21; 2020-12-08)
- MW-1.35-notes
- MW-1.31-release-notes
- Vuln-XSS

Referenced Files

None

Subscribers

- Aklapper
- Daimona
- DannyS712
- dmaza
- gerritbot
- Jdforrester-WMF
- Niharika

View All 11 Subscribers

Description

CVE-2020-35478 - Potential XSS via MediaWiki:blanknamespace outputting Block Logs
CVE-2020-35479 - Potential XSS via the "month messages" such as MediaWiki:january through MediaWiki:december outputting Block Logs

While working on T216940 I have found issues with the BlockLogFormatter

First issue is about the message blanknamespace . it is used with Message::text

```
$namespaces = $params[6]['namespaces'] ?? [];  
$namespaces = array_map( function ( $ns ) {  
    $text = (int)$ns === NS_MAIN  
        ? $this->msg( 'blanknamespace' )->text()  
        : $this->context->getLanguage()->getFormattedNsText( $ns );  
    $params = [ 'namespace' => $ns ];  
  
    return $this->makePageLink( SpecialPage::getTitleFor( 'Allpages' ), $params, $text );  
}, $namespaces );
```

But LogFormatter::makePageLink is documented to get html as third parameter. even in plaintext mode from LogFormatter.

Through that message it is possible to output raw html including script tags.

The second issue is with Language::translateBlockExpiry . The return value is included as raw param in the output without escaping.

```
$durationTooltip = '&lrm;' . htmlspecialchars( $params[4] );  
$blockExpiry = $this->context->getLanguage()->translateBlockExpiry(  
    $params[4],  
    $this->context->getUser(),  
    wfTimestamp( TS_UNIX, $this->entry->getTimestamp() )  
);  
if ( $this->plaintext ) {  
    $params[4] = Message::rawParam( $blockExpiry );  
} else {  
    $params[4] = Message::rawParam(  
        "<span class=\"blockExpiry\" title=\"$durationTooltip\">" .  
        $blockExpiry .  
        "</span>"  
    );  
}
```

Language::translateBlockExpiry itself does not escape all code path, for example the return of Language::userTimeAndDate , which is always unsafe for html.

Through the month messages it is possible to output raw html including script tags.

Taint-check found other places to check, but that looks like false positives to me:

```
13:49:09 includes/logging/BlockLogFormatter.php:98 SecurityCheck-XSS Calling method \Message::rawParams() in \BlockLogFormatter::getMessageParameters that outputs using tainted argument ${arg #1}. (Caused by:  
Builtin->Message::rawParams) (Caused by: includes/logging/BlockLogFormatter.php +82) (Param is raw)  
13:49:09 includes/logging/BlockLogFormatter.php:104 SecurityCheck-XSS Calling method \Message::rawParams() in \BlockLogFormatter::getMessageParameters that outputs using tainted argument ${arg #1}. (Caused by:  
Builtin->Message::rawParams) (Caused by: includes/logging/BlockLogFormatter.php +87) (Param is raw)
```

LogFormatter has a plaintext mode and a normal mode and that confused taint-check

Details

	Project	Subject
P	mediawiki/core	Fixed mixed escaping in Language::translateBlockExpiry
P	mediawiki/core	Fixed mixed escaping in Language::translateBlockExpiry
P	mediawiki/core	Pass escaped html to LogFormatter::makePageLink for sanity
🔴	mediawiki/core	Pass escaped html to LogFormatter::makePageLink for sanity
P	mediawiki/core	Fixed mixed escaping in Language::translateBlockExpiry
P	mediawiki/core	Pass escaped html to LogFormatter::makePageLink for sanity

Customize query in gerrit

Related Objects

Q Search... ▾

Task	Graph	Mentions	Duplicates
Status	Assigned	Task	
✓ Resolved	Reedy	T263002 Release MediaWiki 1.31.11/1.35.1	
🔔 ✓ Resolved	Reedy	T263003 Tracking bug for MediaWiki 1.31.11/1.35.1	
✓ Resolved	Umherirrender	T269930 BlockLogFormatter can output raw html (CVE-2020-35478, CVE-2020-35479)	

🔧 Umherirrender created this task. 2020-11-29 11:17:31 (UTC+0)

👤 Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2020-11-29 11:17:33 (UTC+0)

🔗 Reedy added projects: **MediaWiki-Blocks**, **MediaWiki-Logevents**. 2020-11-29 16:59:26 (UTC+0)

🔧 Reedy updated the task description. ([Show Details](#))

➡ Reedy triaged this task as *High* priority. 2020-11-30 16:24:12 (UTC+0)

📋 Reedy moved this task from **Incoming** to **Watching** on the **Security-Team** board.

🔗 Tchanders added a project: ~~Anti-Harassment (The Letter Song)~~. 2020-12-07 14:46:14 (UTC+0)

👤 Tchanders added subscribers: **dmaza**, **STran**, **Niharika**.

📋 Tchanders moved this task from **Ready** (**ONLY IF YOU HAVE NO MORE CODE TO REVIEW**) to **Code Review** on the ~~Anti-Harassment (The Letter Song)~~ board. 2020-12-07 16:13:34 (UTC+0)

Umherirrender claimed this task. 2020-12-07 17:19:06 (UTC+0) ▾

First part fixed with <https://gerrit.wikimedia.org/r/c/mediawiki/core/+646684>

Second part fixed with <https://gerrit.wikimedia.org/r/c/mediawiki/core/+646689>

Could be public after the next train

🔗 Jdforrester-WMF added a project: ~~MW 1.36 notes (1.36.0-wmf.21, 2020-12-09)~~. 2020-12-07 17:21:07 (UTC+0)

🔗 sbassett added a parent task: ~~T263003: Tracking bug for MediaWiki 1.31.11/1.35.1~~. 2020-12-07 17:24:42 (UTC+0)

📋 Tchanders moved this task from **Code Review** to **Done: Q2 (2020-2021)** on the **Anti-Harassment (The Letter Song)** board. 2020-12-08 15:33:14 (UTC+0)

👤 Tchanders added subscribers: **DannyS712**, **Jdforrester-WMF**, **Tchanders**.

We'll keep an eye on this, but looks like there's nothing for **Anti-Harassment** to do, thanks to , and sorting it quickly!

🔗 Reedy mentioned this in ~~T263003: Tracking bug for MediaWiki 1.31.11/1.35.1~~. 2020-12-15 13:28:18 (UTC+0)

👤 Reedy added a subscriber: **gerritbot**.

gerritbot added a comment. 2020-12-15 13:37:16 (UTC+0) ▾

Change 649521 had a related patch set uploaded (by Reedy; owner: Umherirrender):
[mediawiki/core@REL1_35] Pass escaped html to LogFormatter::makePageLink for sanity

<https://gerrit.wikimedia.org/r/649521>

gerritbot added a project: **Patch-For-Review**. 2020-12-15 13:37:20 (UTC+0) ▾

Change 649522 had a related patch set uploaded (by Reedy; owner: Umherirrender):
[mediawiki/core@REL1_31] Pass escaped html to LogFormatter::makePageLink for sanity

<https://gerrit.wikimedia.org/r/649522>

gerritbot added a comment. 2020-12-15 13:38:16 (UTC+0) ▾

Change 649522 **abandoned** by Reedy:
[mediawiki/core@REL1_31] Pass escaped html to LogFormatter::makePageLink for sanity

Reason:

<https://gerrit.wikimedia.org/r/649522>


gerritbot added a comment. 2020-12-15 13:40:10 (UTC+0) ▾


Change 649523 had a related patch set uploaded (by Reedy; owner: Umherirrender):
[mediawiki/core@REL1_35] Fixed mixed escaping in Language::translateBlockExpiry

https:// Gerrit Wikimedia.org/r/649523	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-15 13:40:56 (UTC+0)</div></div></div></div>	
<div>Change 649524 had a related patch set uploaded (by Reedy; owner: Umherirrender): [mediawiki/core@REL1_31] Fixed mixed escaping in Language:translateBlockExpiry https:// Gerrit Wikimedia.org/r/649524</div>	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-15 13:46:48 (UTC+0)</div></div></div></div>	
<div>Change 649524 abandoned by Reedy: [mediawiki/core@REL1_31] Fixed mixed escaping in Language:translateBlockExpiry Reason: https:// Gerrit Wikimedia.org/r/649524</div>	
<div><div><div><div></div><div>Reedy added a subscriber: Reedy.</div><div>2020-12-15 13:47:03 (UTC+0)</div></div></div></div>	
<div>Looks like the first patch (https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646684) isn't relevant for REL1_31, or code has been moved around/refactored (ie it needs patching elsewhere)... And for https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646689, at least for BlockLogFormatter.php, again, the same? What about the two <code>trim()</code> calls in <code>Language</code> ? They seem a bit superfluous by themselves At least some of the touched code is from 1.33.0+ in <code>rMW31ba7a3e5c6f: Fix malformed output of block logs</code> ... And then various supporting changes from before that Thoughts?</div>	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-15 13:51:27 (UTC+0)</div></div></div></div>	
<div>Change 649521 merged by jenkins-bot: [mediawiki/core@REL1_35] Pass escaped html to LogFormatter::makePageLink for sanity https:// Gerrit Wikimedia.org/r/649521</div>	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-15 13:53:11 (UTC+0)</div></div></div></div>	
<div>Change 649523 merged by jenkins-bot: [mediawiki/core@REL1_35] Fixed mixed escaping in Language:translateBlockExpiry https:// Gerrit Wikimedia.org/r/649523</div>	
<div><div><div><div></div><div>Reedy mentioned this in T203009: Obtain CVEs for 1.31.11/1.35.1 security releases.</div><div>2020-12-15 14:03:30 (UTC+0)</div></div></div></div>	
<div><div><div><div></div><div>Reedy removed a project: Patch-For-Review.</div><div>2020-12-15 16:18:12 (UTC+0)</div></div></div></div>	
<div><div><div><div></div><div>Jdforrester-WMF added projects: MW-1.35-notes, MW-1.31-release-notes.</div><div>2020-12-15 16:35:07 (UTC+0)</div></div></div></div>	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-16 12:51:33 (UTC+0)</div></div></div></div>	
<div>Change 649524 restored by Reedy: [mediawiki/core@REL1_31] Fixed mixed escaping in Language:translateBlockExpiry https:// Gerrit Wikimedia.org/r/649524</div>	
<div><div><div><div></div><div>Reedy added a comment.</div><div>Edited · 2020-12-16 12:56:32 (UTC+0)</div></div></div></div>	
<div><div><div><div></div><div>In T206930#6691979, @Reedy wrote: Looks like the first patch (https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646684) isn't relevant for REL1_31, or code has been moved around/refactored (ie it needs patching elsewhere)... And for https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646689, at least for BlockLogFormatter.php, again, the same? What about the two <code>trim()</code> calls in <code>Language</code> ? They seem a bit superfluous by themselves At least some of the touched code is from 1.33.0+ in <code>rMW31ba7a3e5c6f: Fix malformed output of block logs</code> ... And then various supporting changes from before that Thoughts?</div></div><div><div>Ok. So the first patch, ala https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646684 was not added till 1.33 in <code>rMW85c91cfbf09d: Add namespace restrictions to block's log messages</code> for <code>T204985: Update block logs with namespace block details</code>. I'm declaring that as not applicable for 1.31. https:// Gerrit Wikimedia.org/r/c/mediawiki/core/+646689 goes on top of <code>rMW31ba7a3e5c6f: Fix malformed output of block logs</code> for T208523: Blocks log entries display as malformed on Special:CheckUser also last changed in 1.33. But that only added "plaintext" support. The code being fixed is still there though Will bring it in, with the refactoring to move the <code>translateBlockExpiry</code> call also into a variable to keep the code similar. Not doing a full backport of that patch (<code>rMW31ba7a3e5c6f: Fix malformed output of block logs</code>), as I don't think it's particularly warranted</div></div></div></div>	
<div><div><div><div></div><div>Reedy closed this task as <i>Resolved</i>.</div><div>2020-12-16 13:04:15 (UTC+0)</div></div></div></div>	
<div>Need to get a CVE for this one</div>	
<div><div><div><div></div><div>gerritbot added a comment.</div><div>2020-12-16 13:09:32 (UTC+0)</div></div></div></div>	
<div>Change 649524 merged by jenkins-bot: [mediawiki/core@REL1_31] Fixed mixed escaping in Language:translateBlockExpiry https:// Gerrit Wikimedia.org/r/649524</div>	
<div><div><div><div></div><div>Reedy renamed this task from <i>BlockLogFormatter can output raw html</i> to <i>BlockLogFormatter can output raw html</i> (CVE-2020-35478, CVE-2020-35479).</div><div>2020-12-16 19:57:39 (UTC+0)</div></div></div></div>	
<div><div><div><div></div><div>Reedy updated the task description. (Show Details)</div></div></div></div>	

This needed two different CVE, because two different CVEs.


Might need to do some upstream tweaking post release.

 **Reedy** changed the visibility from "**Custom Policy**" to "Public (No Login Required)". 2020-12-18 00:24:47 (UTC+0)

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

 **sbassett** added a project: **Vuln-XSS**. 2021-03-16 21:30:53 (UTC+0)

 **Zabe** merged a task: ~~**7250612: Language::translateBlockExpiry escapes HTML inconsistently.**~~ 2021-06-24 11:57:51 (UTC+0)

 **Zabe** added a subscriber: **Daimona**.

 **sbassett** moved this task from **Watching** to **Our Part Is Done** on the **Security-Team** board. 2021-06-24 18:11:51 (UTC+0)