

✓ CVE-2021-35197: Blocked users should not be able to issue purges (action=purge)

✓ Closed, Resolved

🌐 Public

SECURITY

Actions

Assigned To

Reedy

Authored By

Legoktm

2021-04-15 08:37:57 (UTC+0)

Tags

👤 Security-Team (Watching)

🔒 Security

🔒 Vuln-DoS (Tracked)

📦 MediaWiki-Blocks (Backlog)

📦 MediaWiki-Action-API (Unsorted)

📍 Sustainability (Incident Followup)

🔒 SecTeam-Processed (Completed)

🔒 Vuln-MissingAuthz (Tracked)

🔒 Patch-For-Review

📄 MW-1.35-notes

📄 MW-1.36-notes (Backlog)

📄 MW-1.31-release-notes

📍 MW-1.37-notes (1.37.0-wmf.12; 2021-06-28)

Referenced Files

📄 F34400119: T280226.patch

2021-04-15 12:04:28 (UTC+0)

Subscribers

Aklapper

Armando805ox

DannyS712

gerritbot

IN

jcrespo

Legoktm

View All 13 Subscribers

Tokens

Description

I blocked a misbehaving bot on-wiki and it was still able to send purges via the API until its IP range was blocked through varnish. I expect that an account that is sitewide blocked is unable to issue purges via the API or index.php.

Details

Project	Subject
📄 mediawiki/core	SECURITY: Prevent blocked users from purging pages
📄 mediawiki/core	SECURITY: Prevent blocked users from purging pages
📄 mediawiki/core	SECURITY: Prevent blocked users from purging pages
📄 mediawiki/core	SECURITY: Prevent blocked users from purging pages

Customize query in gerrit

Related Objects

🔍 Search... ▼

Task Graph	Mentions	
Status	Assigned	Task
✓ Resolved	Reedy	🔒279725 Release MediaWiki 1.31.15/1.35.3/1.36.1
🔒 ✓ Resolved	Reedy	🔒279726 Tracking bug for MediaWiki 1.31.15/1.35.3/1.36.1
✓ Resolved	Reedy	🔒280226 CVE-2021-35197: Blocked users should not be able to issue purges (action=purge)

- 🔧 Legoktm created this task. 2021-04-15 08:37:57 (UTC+0)
- 👤 🛡️ Restricted Application added a subscriber: Aklapper. · View Herald Transcript 2021-04-15 08:37:58 (UTC+0)
- 🔗 Legoktm added projects: Vuln-DoS, MediaWiki-Blocks, MediaWiki-Action-API. 2021-04-15 08:39:00 (UTC+0)
- 👤 jcrespo awarded a token. 2021-04-15 08:55:28 (UTC+0)
- 🔗 jcrespo added projects: Wikimedia-production-error, Sustainability (Incident Followup). 2021-04-15 09:22:41 (UTC+0)
- 👤 jcrespo added a subscriber: jcrespo.

Public incident ticket: **T260232**

 Reedy added a subscriber: **Reedy**. 2021-04-15 11:58:03 (UTC+0)

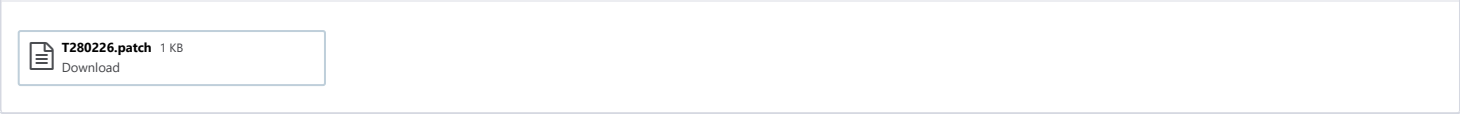
Fix to PurgeAction is very trivial... Just remove the `requiresUnblock` override.

Api is similarly easy, just re-use the code from ApiTag

```
// Fail early if the user is sitewide blocked.
$block = $user->getBlock();
if ( $block && $block->isSitewide() ) {
    $this->dieBlocked( $block );
}
```

Patch incoming.

Reedy added a comment. 2021-04-15 12:04:28 (UTC+0)

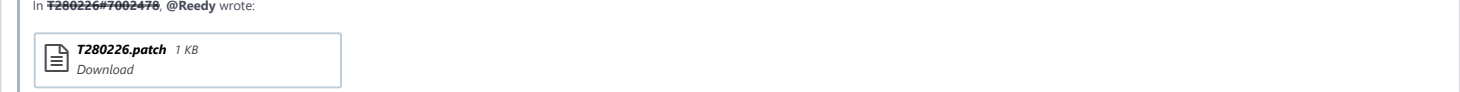


Reedy added a project: **SecTeam-Processed**. 2021-04-15 14:23:25 (UTC+0)

📌 Reedy moved this task from **Incoming** to **In Progress** on the **Security-Team** board.

 Krinkle removed a project: **Wikimedia-production-error**. 2021-04-15 19:37:01 (UTC+0)

Legoktm added a comment. 2021-04-16 04:26:04 (UTC+0)

[illegible]

sbassett moved this task from In Progress to Security Patch To Deploy on the Security-Team board. 2021-04-16 16:06:05 (UTC+0)

sbassett added a subscriber: sbassett. 2021-04-19 21:05:56 (UTC+0)

Deployed to wmf.1. Also updated on T276237.

→ sbassett triaged this task as Low priority. 2021-04-19 21:06:47 (UTC+0)

sbassett moved this task from Security Patch To Deploy to Our Part Is Done on the Security Team board

- sbassett moved this task from Security Patch to Deploy to Our Part is Done on the Security-Team board.
-  sbassett added a project: Vuln-MissingAuthz.

sbassett added a parent task: ~~T279726~~ [Tracking bug for MediaWiki 1.31.15/1.35.3/1.36.1](#).

 sbassett moved this task from **Our Part Is Done** to **Watching** on the **Security-Team** board. 2021-05-17 18:34:06 (UTC+0)

Reedy added a comment. Edited · 2021-06-22 12:39:33 (UTC+0)

Plan is to get this out this week (well, tomorrow). So this patch will apply fine to 1.35 and 1.36 straight off.

For 1.31, the `isSiteWide` wasn't added till 1.33... The change to `PurgeAction` is fine and can be applied as is.

We could just use any block... Which seems probably the simplest way forward, as 1.31 has no concept of these other "types" of blocks, and is due to become EOL this month... But is being extended for one more quarter to meet our LTS overlap requirements.

```
// Fail early if the user is blocked.
$block = $user->getBlock();
if ( $block ) {
    $this->dieBlocked( $block );
}
```

6 Reedy mentioned this in [1475732: Obtain CVEs for 1.5.1.15/1.5.5.3/1.5.6.1 security releases](#). 2021-06-22 12:50:15 (UTC+0)

👤 Reedy claimed this task. 2021-06-22 12:53:04 (UTC+0)

🔧 Reedy renamed this task from *Blocked users should not be able to issue purges (action=purge)* to *CVE-2021-35197: Blocked users should not be able to issue purges (action=purge)*. 2021-06-22 13:00:07 (UTC+0)

 Reedy added a subscriber: **gerritbot**. 2021-06-22 13:04:04 (UTC+0)

sbassett added a comment. 2021-06-22 15:21:51 (UTC+0)

```
+1 for if (any block exists)
```


















● Legoktm added a comment. 2021-06-22 17:24:34 (UTC+0)

+1 on that approach from me as well.

● [gerrithot](#) added a comment 2021-06-23 16:20:57 (UTC +0)

Change 701143 had a related patch set uploaded (by Reedy; author: Reedy):

[mediawiki/core@REL1_31] SECURITY: Prevent blocked users from purging pages

https:// Gerrit.wikimedia.org/r/701143	
 gerritbot added a project: Patch-For-Review . 2021-06-23 16:20:59 (UTC+0)	▼
Change 701146 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@REL1_35] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701146	
 gerritbot added a comment. 2021-06-23 16:22:02 (UTC+0)	▼
Change 701150 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@REL1_36] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701150	
 gerritbot added a comment. 2021-06-23 16:22:27 (UTC+0)	▼
Change 701153 had a related patch set uploaded (by Reedy; author: Reedy): [mediawiki/core@master] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701153	
 gerritbot added a comment. 2021-06-23 16:32:27 (UTC+0)	▼
Change 701143 merged by jenkins-bot: [mediawiki/core@REL1_31] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701143	
 Reedy closed this task as Resolved . 2021-06-23 16:33:56 (UTC+0)	
 gerritbot added a comment. 2021-06-23 16:42:57 (UTC+0)	▼
Change 701146 merged by jenkins-bot: [mediawiki/core@REL1_35] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701146	
 gerritbot added a comment. 2021-06-23 16:47:38 (UTC+0)	▼
Change 701150 merged by jenkins-bot: [mediawiki/core@REL1_36] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701150	
 Reedy changed the visibility from " Custom Policy " to "Public (No Login Required)". 2021-06-23 16:56:17 (UTC+0)	
 Reedy changed the edit policy from " Custom Policy " to "All Users".	
 gerritbot added a comment. 2021-06-23 16:58:28 (UTC+0)	▼
Change 701153 merged by jenkins-bot: [mediawiki/core@master] SECURITY: Prevent blocked users from purging pages https:// Gerrit.wikimedia.org/r/701153	
 ReleaseTaggerBot added projects: MW-1.35-notes , MW-1.36-notes , MW-1.34-release-notes , MW-1.37-notes (1.37.0-wmf.12 , 2021-06-20). 2021-06-23 17:00:30 (UTC+0)	
 TheresNoTime added a subscriber: TheresNoTime . 2021-08-14 23:23:25 (UTC+0)	
 IN mentioned this in 7292198: Allow a user to be blocked from purge pages only . 2021-09-30 13:29:44 (UTC+0)	
 Armando805ox added a subscriber: Armando805ox . 2021-10-17 11:09:27 (UTC+0)	
 DannyS712 merged a task:  Restricted Task. 2022-05-29 08:09:13 (UTC+0)	
 DannyS712 added subscribers: IN , taavi , Zabe and 2 others .	