CUNY Academic Commons - Support #14404

blocked IP of user?

2021-05-02 10:14 AM - Marilyn Weber

Status:	Resolved	**Start date:**	2021-05-02
Priority name:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category name:		**Estimated time:**	0.00 hour
Target version:	Not tracked		

Description

via ZendDesk:

"
I am managing a few Commons Wordpress and somehow my home IP address (207.38.251.155) has been blocked by the server. When you have a chance, could you please add it to the white list?
Here is the list of the pages that I manage:
https://asianheritage.commons.gc.cuny.edu
https://chrysanthemum.commons.gc.cuny.edu
https://tokyo2021.commons.gc.cuny.edu
https://japanese.commons.gc.cuny.edu
Thank you so much,
Tomonori
Tomonori Nagano, Ph.D."

History

#1 - 2021-05-02 08:41 PM - Marilyn Weber

I asked if she was able to log in at all. No - "I cannot access https://commons.gc.cuny.edu at all. I am sure that the server is up, but I lost my access to the server. As I understand, it happens if my IP is blocked by some security plug in (Jetpack, WP Security etc). I was updating multiple posts on one of the sites yesterday and it might have put my IP on the IP block list."

#2 - 2021-05-03 11:05 AM - Boone Gorges

In the access logs, I see successful requests up through 01/May/2021:19:58:02. Can I assume that the failed requests all happened after this time?

I've sent an inquiry to IT.

#3 - 2021-05-03 11:58 AM - Boone Gorges

- Status changed from New to Reporter Feedback

I heard back from IT. The IP address is, in fact, blocked. Activity from the IP address triggered a rule at the firewall. The pattern appears to be a large number of requests by the MarsEdit blogging software. Could you please pass the following requests for information along to the user:

- Can you confirm that you were using MarsEdit to manage content at asianheritage.commons.gc.cuny.edu between 6-7pm EDT on May 1?
- Assuming "yes", can you confirm the kinds of activity you were performing? Specifically, were you doing anything that might have triggered abnormally large numbers of requests to the Commons site? For example, were you editing or deleting large numbers of posts?
- Are there configuration settings in MarsEdit that might control the number of requests that MarsEdit makes to the server? For example, does it have "auto-save" functionality built in? Or does it have settings that control how the software fetches content from the blog?

#4 - 2021-05-03 12:44 PM - Marilyn Weber

She replies "yes, I am using MarsEdit for my WordPress sites, including asianheritage.commons.gc.cuny.edu< http://asianheritage.commons.gc.cuny.edu>.

As I mentioned in my initiative e-mail, I was migrating our blog posts from another site (Facebook) into the Commons WordPress, which must have triggered a red flag. I believe I had to move about 40 posts on Friday and my access was blocked. I usually post only a few posts a week and I have been using MarsEdit for a few years, so I believe it has nothing to do with its configuration."

#5 - 2021-05-03 03:48 PM - Boone Gorges

Thanks for the update. I've passed this information along to IT, along with a request to remove the IP from the block list. I'll be back in touch when I hear something.

#6 - 2021-05-03 04:38 PM - Marilyn Weber

- File Screen Shot 2021-05-03 at 3.16.50 PM.jpg added

She has it set to 50:

Hello Marilyn,

Yes, there is a way to control how many articles the program fetches at a time. I attached the screenshot. I can lower it to a smaller number, if necessary.

Tomonori

#7 - 2021-05-03 09:28 PM - Marilyn Weber

Just out of curiosity, was it moving so many posts at once? Should she stop using MarsEdit altogether? (Or are we waiting for IT to make this all clear?)

#8 - 2021-05-04 10:15 AM - Boone Gorges

It's a combination of MarsEdit and the fact that so many posts are being moved.

MarsEdit uses the XML-RPC protocol to communicate with WordPress. This protocol is a common vector for various kinds of brute-force attacks against WordPress installations, so our firewall software is configured to detect and block clients that make large numbers of requests to the XML-RPC endpoint. Under normal use - writing blog posts, etc - MarsEdit contacts the server only occasionally. But when "moving" or editing large numbers of posts consecutively, MarsEdit makes many requests, triggering the firewall rules.

MarsEdit should be fine for normal use. I'd recommend that users who need to make more administrative changes, including bulk post edits, instead use the WordPress web interface (wp-admin), where you won't run into the same firewall issues.

I'm still waiting for confirmation about the IP address. If the user tests and discovers that the block has been lifted, please let me know so I can close this ticket out.

#9 - 2021-05-07 09:08 AM - Marilyn Weber

She's still blocked. Any word from IT?

#10 - 2021-05-07 09:52 AM - Boone Gorges

No word. I've just followed up. Extend our apologies for the delay. I'll be in touch as soon as I hear something.

#11 - 2021-05-10 12:59 PM - Marilyn Weber

She reports that the block is lifted. Thanks!

#12 - 2021-05-10 01:00 PM - Boone Gorges

- Status changed from Reporter Feedback to Resolved

- Target version set to Not tracked

Great, thanks for confirming!

Files

Screen Shot 2021-05-03 at 3.16.50 PM.jpg	68.5 KB	2021-05-03	Marilyn Weber