

mw-ext-FileImporter uses a WMF IP address, does not include XFF for users using this extension (CVE-2020-27621)

Closed, ResolvedPublicSECURITY

Actions

Assigned To

thiemowmde

Authored By

Risker

2020-10-18 04:46:36 (UTC+0)

Tags

Security-Team

 (Our Part Is Done)

Security

Move-Files-To-Commons

 (Tickets in sprint)

Unplanned-Sprint-Work

WMDE-QWERTY-Sprint-2020-10-07

 (Done)

MW-1.36-notes

 (1.36.0-wmf.13; 2020-10-12)

Vuln-Misconfiguration

 (Tracked)

Referenced Files

None

Subscribers

Aklapper

AmandaNP

Andrew-WMDE

awight

jrb

Lea_WMDE

Lena_WMDE

View All 16 Subscribers

Description

Identified this issue when checkusering a suspicious account; one of the IPs the account used was mw-ext-FileImporter, and at first glance it looked like it was some sort of shared IP because the "readout" on the CU result said:

- 2620:0:860:2:208:80:153:61 (block) (16:40, 21 September 2020 -- 03:33, 12 October 2020) [35] (~2,288 from all users)
- Check of the IP revealed that it ends every CU log entry with IP: 2620:0:860:2:208:80:153:61 mw-ext-FileImporter/* (<https://www.mediawiki.org/wiki/Extension:FileImporter>)

This is a problem.

*First, it doesn't give the XFF or true IP address of the person using the extension. It is acting essentially as an open proxy.

*Second, it's not restricted in its use to people with File Mover permission. The account I was checking does not have that permission.

*Third, if someone who used this extension recently got blocked with "autoblock" selected (as is standard on English Wikipedia), it would cause cascading blocks to every other user who tried to use the extension during the block period, until we figured out what was happening. It would essentially disable this extension on English Wikipedia.

Not sure how this wasn't noticed/reported before. But I was doing the Checkuser with the expectation that I would be blocking the account involved, and this was a close call. It is only a matter of luck that it hasn't happened already.

Details

Author Affiliation

Wikimedia Communities

Project	Subject
mediawiki/extensions/FileImporter	Set originalRequest (incl. X-Forwarded-For) for remote edits
mediawiki/extensions/FileImporter	Set originalRequest (incl. X-Forwarded-For) for remote edits
mediawiki/extensions/FileImporter	Set originalRequest (incl. X-Forwarded-For) for remote edits
mediawiki/extensions/FileImporter	Set originalRequest (incl. X-Forwarded-For) for remote edits

Customize query in gerrit

Related Objects

Q Search...

Task Graph

Mentions

Status

Assigned

Task

Restricted Task

Resolved

thiemowmde

T265810 mw-ext-FileImporter uses a WMF IP address, does not include XFF for users using this extension (CVE-2020-27621)

Risker created this task.

2020-10-18 04:46:36 (UTC+0)

Restricted Application added a subscriber: Aklapper.

View Herald Transcript

2020-10-18 04:46:37 (UTC+0)

SQL added a comment.

2020-10-18 04:48:42 (UTC+0)

Non-ideal at best. This should report the user's address. https://whois.toolforge.org/gateway.py?lookup=true&ip=2620%3A0%3A860%3A2%3A208%3A80%3A153%3A61	
Aklapper added a project: Move-Files-To-Commons . 2020-10-18 09:50:41 (UTC+0)	
Urbanecm added subscribers: Lea_WMDE , awight , Lena_WMDE , Urbanecm . 2020-10-18 11:02:17 (UTC+0)	
Adding few people from WMDE based on https://phabricator.wikimedia.org/project/members/2671/ .	
Tks4Fish added a subscriber: Tks4Fish . 2020-10-18 12:40:20 (UTC+0)	
Risker added a subscriber: AmandaNP . 2020-10-18 19:02:02 (UTC+0)	
<i>This comment was removed by Risker.</i>	
AmandaNP added a parent task: Restricted Task. 2020-10-18 19:06:09 (UTC+0)	
awight added subscribers: Andrew-WMDE , lilients_WMDE . 2020-10-19 13:06:14 (UTC+0)	
Reedy moved this task from Incoming to Watching on the Security-Team board. 2020-10-19 15:26:24 (UTC+0)	
awight added subscribers: thiemowmde , WMDE-Fisch . 2020-10-20 09:05:01 (UTC+0)	
awight added projects: Unplanned-Sprint-Work , WMDE-QWERTY-Sprint-2020-10-07 . 2020-10-20 10:15:09 (UTC+0)	
thiemowmde moved this task from Backlog to Tickets in sprint on the Move-Files-To-Commons board. 2020-10-20 10:42:40 (UTC+0)	
<div><div>@Risker</div>, thanks for the report. Based on the idea that an <code>X-Forwarded-For</code> header might be missing somewhere, we reviewed the FileImporter's workflow. So far we can think of only one place that might be related: when FileImporter does an remote edit to mark the file on the source wiki as <code>{{NowCommons}}</code>. I created a proof-of-concept patch at https://gerrit.wikimedia.org/r/635265. Unfortunately we aren't able to confirm this at the moment. No team member does have CheckUser rights. Can you point us to a revision ID that was attributed to this awkward FileImporter IP?</div>	
Urbanecm added a comment. Edited · 2020-10-20 11:37:02 (UTC+0)	
<div><div>@thiemowmde</div> As long as originalRequest will add the header, your patch seems to be correct. You can find a list of five examples at P13028 (NDA-only paste; you can subscribe other WMDE staff if needed; note almost all pages are deleted, happy to screenshot the history if needed).</div>	
thiemowmde added a comment. 2020-10-20 12:09:40 (UTC+0)	
Awesome, thanks! I don't want to past a user or file name here. But the list confirms this is indeed about the remote edits that mark the source file as being moved to commons. The summary line for all edits in question is <code>This file is now on Wikimedia Commons at https://commons.wikimedia.org/wiki/File:...</code> (moved with <code>FileImporter</code>).	
Lena_WMDE moved this task from Sprint Backlog to Doing on the WMDE-QWERTY-Sprint-2020-10-07 board. 2020-10-20 12:14:18 (UTC+0)	
thiemowmde claimed this task. 2020-10-20 12:22:59 (UTC+0)	
thiemowmde moved this task from Doing to Review on the WMDE-QWERTY-Sprint-2020-10-07 board.	
Note the patch will fix this only for future edits. Edits already in the <code>cuc_ip</code> database table will still contain a wrong IP address. Please let us know if you think this is a problem that needs fixing.	
Urbanecm added a comment. 2020-10-20 12:32:45 (UTC+0)	
<div><div>@thiemowmde</div> I don't think you can fix it - the IP isn't stored anywhere now.</div>	
Urbanecm added a comment. 2020-10-20 13:08:17 (UTC+0)	
<div><div>/me impersonates gerritbot</div><div>Change 635265 approved by Urbanecm: [mediawiki/extensions/FileImporter@master] Set originalRequest (incl. X-Forwarded-For) for remote edits https://gerrit.wikimedia.org/r/635265</div></div>	
Urbanecm added a comment. 2020-10-20 13:26:48 (UTC+0)	
<div><div>/me impersonates gerritbot</div><div>Change 635265 merged by jenkins-bot: [mediawiki/extensions/FileImporter@master] Set originalRequest (incl. X-Forwarded-For) for remote edits https://gerrit.wikimedia.org/r/635265 Change 635039 had a related patch set uploaded (by Urbanecm; owner Urbanecm): [mediawiki/extensions/FileImporter@wmf/1.36.0-wmf.13] Set originalRequest (incl. X-Forwarded-For) for remote edits https://gerrit.wikimedia.org/r/635039 Change 635040 had a related patch set uploaded (by Urbanecm; owner Urbanecm): [mediawiki/extensions/FileImporter@wmf/1.36.0-wmf.14] Set originalRequest (incl. X-Forwarded-For) for remote edits https://gerrit.wikimedia.org/r/635040</div></div>	
thiemowmde mentioned this in rEFLlff0ec0ac1ce5: Set originalRequest (incl. X-Forwarded-For) for remote edits . 2020-10-20 13:31:08 (UTC+0)	
Urbanecm mentioned this in rEFLl5f8d3de14c11: Set originalRequest (incl. X-Forwarded-For) for remote edits . 2020-10-20 14:00:04 (UTC+0)	
Urbanecm mentioned this in rEFLl5eee9b773338: Set originalRequest (incl. X-Forwarded-For) for remote edits . 2020-10-20 14:46:07 (UTC+0)	
Urbanecm closed this task as Resolved . 2020-10-20 14:48:21 (UTC+0)	

I've deployed the change. Should work fine now.

 Jdforrester-WMF added a project: ~~MW-1.36-notes (1.36.0-wmf.16, 2020-11-03)~~. 2020-10-20 15:00:05 (UTC+0)

 Urbanecm edited projects, added ~~MW-1.36-notes (1.36.0-wmf.13, 2020-10-12)~~, removed ~~MW-1.36-notes (1.36.0-wmf.16, 2020-11-03)~~. 2020-10-20 15:02:44 (UTC+0) 

Adding wmf.13 tag, because this is deployed as-of wmf.13.

→ sbasett triaged this task as *Low* priority. 2020-10-20 16:12:25 (UTC+0)

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

 sbasett mentioned this in ~~T263810: Write and send supplementary release announcement for extensions and skins with security patches (1.31.11/1.35.1)~~.

 sbasett moved this task from **Watching to Our Part Is Done** on the **Security-Team** board. 2020-10-20 16:14:26 (UTC+0)

 gerritbot added a comment. 2020-10-20 16:15:41 (UTC+0) 


Change 635328 had a related patch set uploaded (by Urbanecm; owner: Thiemo Kreuz (WMDE)):
[mediawiki/extensions/FileImporter@REL1_35] Set originalRequest (incl. X-Forwarded-For) for remote edits
<https://gerrit.wikimedia.org/r/635328>

 gerritbot added a comment. 2020-10-20 21:37:19 (UTC+0) 

Change 635328 **merged** by jenkins-bot:
[mediawiki/extensions/FileImporter@REL1_35] Set originalRequest (incl. X-Forwarded-For) for remote edits
<https://gerrit.wikimedia.org/r/635328>

 thiemowmde mentioned this in rEFLla3f025ff07ad: Set originalRequest (incl. X-Forwarded-For) for remote edits. 2020-10-20 21:39:53 (UTC+0)

 thiemowmde moved this task from **Review** to **Done** on the ~~WMDE-OWERTY-Sprint-2020-10-07~~ board. 2020-10-21 07:05:01 (UTC+0)

 sbasett renamed this task from *mw-ext-FileImporter uses a WMF IP address, does not include XFF for users using this extension* to *mw-ext-FileImporter uses a WMF IP address, does not include XFF for users using this extension (CVE-2020-27621)*.
2020-10-22 20:28:10 (UTC+0)

 sbasett added a project: **Vuln-Misconfiguration**. 2021-03-16 21:29:59 (UTC+0)

 RhinosF1 added a subscriber: **RhinosF1**. 2021-03-16 21:32:16 (UTC+0)