

New issue

[Jump to bottom](#)

## uploading SVG images fails #68

🔒 Closed

pierstitus opened this issue on Apr 3, 2017 · 9 comments

Labels

enhancement

pierstitus commented on Apr 3, 2017

Contributor

- flagrow/upload extension version: 4.11
- flarum version: 0.1.0-beta.6
- Upload adapter causing issues: local

Uploading SVG images fails when they are opened by the image processor. I didn't test it but looking at the code I guess also uploading any image file other than png, jpeg or gif would fail.

I think the following lines should be changed:

src/Listeners/ProcessesImages.php:

```
--- a/src/Listeners/ProcessesImages.php
+++ b/src/Listeners/ProcessesImages.php
@@ -43,7 +43,7 @@ class ProcessesImages

    protected function validateMime($mime)
    {
-        if (Str::startsWith($mime, 'image/')) {
+        if ($mime == 'image/jpeg' || $mime == 'image/png' || $mime == 'image/gif' || $mime ==
'image/svg+xml') {
            return true;
        }
```

src/Processors/ImageProcessor.php:

```
--- a/src/Processors/ImageProcessor.php
+++ b/src/Processors/ImageProcessor.php
```


```
@@ -43,7 +43,8 @@ class ImageProcessor implements Processable
    */
    public function process(File &$file, UploadedFile &$upload)
    {
-        if ($upload->getMimeType() != 'image/gif') {
+        $mimeType = $upload->getMimeType();
+        if ($mimeType == 'image/jpeg' || $mimeType == 'image/png') {
            $image = (new ImageManager())->make($upload->getRealPath());

            if ($this->settings->get('mustResize')) {
```

luceos commented on Apr 3, 2017 • edited ▼

Collaborator

Good point, allowing svg is a must have! Feel free to do a PR (you can even do this with the Github editor).

  **luceos** added the **enhancement** label on Apr 3, 2017

jtojnar commented on Apr 3, 2017

Contributor

I love SVGs but they also bring wide range of vulnerabilities. When inserted as an image, the contained scripts will not be executed but once the image is uploaded on the server, user just needs to be convinced to visit the link for havoc to be wrought.

  **pierstitus** mentioned this issue on Apr 4, 2017

**fix handling of svg and unsupported image types (fixes #68) #70**

 Merged

pierstitus commented on Apr 4, 2017

Contributor

Author

With great features come vulnerabilities, but that should be decided by the forum admin by allowing the svg mimetype or not. It would be nice though to be able to choose whether images are inserted as images or as links.

jtojnar commented on Apr 4, 2017

Contributor

I agree that admins should have say in this but if `flagrow/upload` is striving to be a secure software, it should

1. inform the user about [possible consequences](#), and
2. try to mitigate the risk (at least by using [SVG sanitizer](#)).

Either way, security minefields should not be enabled by default.

luceos commented on Apr 4, 2017

Collaborator

@jtojnar thanks for that link I think it would make for a great optional add-on feature. A solution for now would be to add a settings input field that would allow configuration of mime types being shown as images. Wouldn't that solve this all together?

jtojnar commented on Apr 4, 2017

Contributor

@luceos Showing the SVGs as images (via `img` tag) is actually safe. The issue occurs when the uploaded file is visited directly.



luceos closed this as completed in [00c75aa](#) on Apr 10, 2017



luceos reopened this on Apr 10, 2017

luceos commented on Apr 10, 2017

Collaborator

I've merged the PR but adding SVG sanitizer makes sense.

sijad commented on Oct 20, 2017

Contributor

maybe it can be possible to force some specified extension (like svg) be download via php with `Content-Disposition: attachment` header. it might be aslo possible achieve same thing using `.htaccess` for Apache.



imorland mentioned this issue on May 24

Clean and validate uploaded SVG files #318

Merged

imorland commented on May 25

Member

Resolved in `1.2.3`



**imorland** closed this as completed on May 25

---

#### Assignees

No one assigned

---

#### Labels

**enhancement**

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

5 participants

