

There some bugs in binary pdfimages in XPDF4.0.4

3 posts • Page 1 of 1

Post Reply 


Search this topic...



huangyh



There some bugs in binary pdfimages in XPDF4.0.4

 Sat Sep 24, 2022 3:18 pm

Hello, I use fuzzer to test binary pdfimages in XPDF4.0.4, and found some crashes. The crash input and the details of running these input all stored the attachments.

These bugs all can result in stack buffer overflow.

The bug1 crashed in function `Object::copy(Object*)` which locates in file `/xpdf-4.04/xpdf/Object.cc:81:8`.

The bug2 crashed in function `gfseek(_IO_FILE*, long, int)` which locates in file `/xpdf-4.04/goo/gfile.cc:733:10`.

The bug3 crashed in function `XRef::fetch(int, int, Object*, int)` which locates in file `/xpdf-4.04/xpdf/XRef.cc:1207:11`.

Credit

CODE: SELECT ALL

```
Yuhang Huang , Jiayuan Zhang, (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)
Xudong Cao, Mengyue Feng (NCNIPC of China, Hexhive)
```

Wanying Cao, Jiayu Zhao (NCNIPC of China)

Thanks for your time.

ATTACHMENTS

[pdfimages_poc.zip](#)

(79.31 KiB) Downloaded 26 times

[crash.zip](#)

(13.72 KiB) Downloaded 22 times



derekn



Re: There some bugs in binary pdfimages in XPDF4.0.4

 Wed Sep 28, 2022 9:45 pm

All three of those are loops in the PDF object structure. I'm working on a more robust loop detector for Xpdf 5.



huangyh



Re: There some bugs in binary pdfimages in XPDF4.0.4

 Thu Sep 29, 2022 5:14 am

Thanks for your approving!



Post Reply 



3 posts • Page **1** of **1**

[< Return to "XpdfReader"](#)

Jump to 

 **Board index**

 [Delete cookies](#) All times are UTC

Powered by [phpBB®](#) Forum Software © phpBB Limited

[Privacy](#) | [Terms](#)