New issue

Jump to bottom

Infinite loop in function get_xref_linear_skipped in pdf.c #17

Closed **chibataiki** opened this issue on Apr 16, 2021 · 2 comments

chibataiki commented on Apr 16, 2021 • edited

Hi,
I found an infinite loop in function `get_xref_linear_skipped` in pdf.c

env:
version: v0.22b commit `af10865`
OS: ubuntu 20.04

If found 'trailer' ,then look backwards for 'xref'. But if there isn't character 'x' backward, the function `get_xref_linear_skipped` will go into an infinite loop.

```
── source:pdf.c+729 ──
   724        return;
   725
   726      /* If we found 'trailer' look backwards for 'xref' */
   727      ch = 0;
   728      while (SAFE_F(fp, ((ch = fgetc(fp)) != 'x')))
              // fp=0x0000ffffffffeea8 → [...] → 0x00000000fbad2488
 → 729        fseek(fp, -2, SEEK_CUR);
   730
   731      if (ch == 'x')
   732      {
   733          xref->start = ftell(fp) - 1;
   734          fseek(fp, -1, SEEK_CUR);
──────────────────────────────────────────
```

poc(zipped):
pdfresurrect_hang_1.zip

To reproduct:

./pdfresurrect [poc]

reporter: chiba of Topsec alphaLab

👍 2

enferex commented on Apr 18, 2021 Owner

Thanks! I have been able to reproduce this and have a potential fix.

enferex commented on Apr 18, 2021 Owner

Should be fixed in `7e35d18`

👍 1

enferex closed this as completed on Apr 18, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants