Stack-buffer-overflow-XRef-getObjectStream #15

Open **Aurorainfinity** opened this issue on Jul 5, 2020 · 0 comments

Aurorainfinity commented on Jul 5, 2020

```
$ gdb ./pdf2xml

(gdb) r 05-Stack-buffer-overflow-XRef-getObjectStream.pdf test.xml
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Syntax Error (593163): Dictionary key must be a name object
Syntax Error (593170): Dictionary key must be a name object

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6e8c80b in ?? () from /usr/lib/x86_64-linux-gnu/libasan.so.2
(gdb) x/5i $rip
=> 0x7ffff6e8c80b:      mov    %ecx,0x8(%rsp)
0x7ffff6e8c80f: mov    %r8d,0x10(%rsp)
0x7ffff6e8c814: mov    (%rax),%eax
0x7ffff6e8c816: test   %eax,%eax
0x7ffff6e8c818: je     0x7ffff6e8d0a0
```

ref:https://github.com/Aurorainfinity/Poc/tree/master/pdf2xml
05-Stack-buffer-overflow-XRef-getObjectStream.pdf

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant