There seems to be a stack overflow vulnerability here, can you take a look, source code： Object::copy

H00K1998

There seems to be a stack overflow vulnerability here, can you take a look, source code: Object::copy

Sat Jun 04, 2022 8:24 am

Hello, I seem to encounter a stack overflow vulnerability in the process of fuzz test (afl++), can you take a look

Enjoy:)

ATTACHMENTS

poc-images.7z
(188.3 KiB) Downloaded 161 times

derekn

Re: There seems to be a stack overflow vulnerability here, can you take a look, source code: Object::copy

Thu Jun 09, 2022 7:58 pm

That's due to an object loop in the PDF file. I'm planning to implement a more robust loop checker in Xpdf 5.