null pointer dereference caused by no-check malloc pointer

cyth

null pointer dereference caused by no-check malloc pointer

Sat Aug 20, 2022 10:03 am

Hello.
I find a npd bug in xpdf 4.04 in FoFiType1C.cc:2393, it may caused by WebFont.cc:198 (a no-check pointer).
It can be triggered by a crafted file in attachment by using pdftohtml.

ATTACHMENTS

npd_poc.zip
(11.43 KiB) Downloaded 38 times

derekn

Re: null pointer dereference caused by no-check malloc pointer

Tue Aug 23, 2022 6:49 pm

I'll have that fixed in the next release.

Thanks for the bug report.

cyth

Re: null pointer dereference caused by no-check malloc pointer

Thu Aug 25, 2022 2:53 am

Thanks for your confirmation.