Closed Issue created 8 months ago by Jieyong Ma

Closed Logic error in function Hints::Hints

Logic error in function Hints::Hints

A logic error in Function Hints::Hints (poppler/Hints.cc) is found with fuzzing.

There is a check after the memory alloc and set the nPages to zero if failed:

```
if (!nObjects || !pageObjectNum || !xRefOffset || !pageLength || !pageOffset || !numSharedObject ||

    error(errSyntaxWarning, -1, "Failed to allocate memory for hints table");

    nPages = 0;

}
```

But at the end of function, there is a direct call to function readTables WITHOUT the check of nPages.

I believe it should be changed to:

```
if (nPages != 0) {

    readTables(str, linearization, xref, secHdlr);

}
```

Otherwise, with the attached poc.pdf, program pdftops will hang for a very long time (days), could be a DoS.

pdftops poc.pdf

Edited 8 months ago by Jieyong Ma

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 1

Hints::readTables: bail out if we run out of file when reading

!1113

When this merge request is accepted, this issue will be closed automatically.

Activity

Jieyong Ma changed the description 8 months ago

Albert Astals Cid mentioned in merge request !1113 (merged) 8 months ago

Albert Astals Cid @aacid · 8 months ago — Owner

That is on purpose, we try to be as flexible as possible when reading

Albert Astals Cid closed via commit 81044c64 8 months ago

Jieyong Ma @jieyongma · 6 months ago — Author

CVE-2022-27337 has been assigned to this issue.

Please register or sign in to reply

Closed **Logic error in function Hints::Hints**