Bug 1899520 (CVE-2020-25725) - CVE-2020-25725 xpdf: sending crafted a PDF document to the pdftops tool could result in DoS

Keywords: Security ×

Status: CLOSED UPSTREAM
Alias: CVE-2020-25725
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: ~~1899521~~ ~~1899522~~ ~~1899523~~
Blocks:
TreeView+ depends on / blocked

Reported: 2020-11-19 13:28 UTC by Michael Kaplan
Modified: 2021-02-17 19:31 UTC (History)
CC List: 2 users (show)
Fixed In Version:
Doc Type: ---
Doc Text: In Xpdf 4.02, SplashOutputDev::endType3Char(GfxState *state) SplashOutputDev.cc:3079 is trying to use the freed `t3GlyphStack->cache`, which causes an `heap-use-after-free` problem. The codes of a previous fix for nested Type 3 characters wasn't correctly handling the case where a Type 3 char referred to another char in the same Type 3 font.
Clone Of:
Environment:
Last Closed: 2020-11-19 17:28:49 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Michael Kaplan 2020-11-19 13:28:55 UTC — Description

In Xpdf 4.02, SplashOutputDev::endType3Char(GfxState *state) SplashOutputDev.cc:3079 is trying to use the freed `t3GlyphStack->cache`, which causes an `heap-use-after-free` problem. The codes of a previous fix for nested Type 3 characters wasn't correctly handling the case where a Type 3 char referred to another char in the same Type 3 font.

Michael Kaplan 2020-11-19 13:28:58 UTC — Comment 1

Acknowledgments:

Name: Mike Zhang (Pangu Lab)

Michael Kaplan 2020-11-19 13:29:00 UTC — Comment 2

External References:

https://forum.xpdfreader.com/viewtopic.php?f=3&t=41915

Michael Kaplan 2020-11-19 13:30:47 UTC — Comment 3

Created xpdf tracking bugs for this issue:

Affects: epel-6 [~~bug 1899523~~]
Affects: epel-7 [~~bug 1899522~~]
Affects: fedora-all [~~bug 1899521~~]

Product Security DevOps Team 2020-11-19 17:28:49 UTC — Comment 4

This CVE Bugzilla entry is for community support informational purposes only as it does not affect a package in a commercially supported Red Hat product. Refer to the dependent bugs for status of those individual community products.

Note
You need to log in before you can comment on or make changes to this bug.