Bug 1947433 (CVE-2021-30469) - CVE-2021-30469 podofo: use-after-free in PoDoFo::PdfVecObjects::Clear() via crafted PDF file

Keywords: Security ×

Status: CLOSED UPSTREAM
Alias: CVE-2021-30469
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: 1947637 ~~1947635~~ ~~1947636~~
Blocks: 1947624
TreeView+ depends on / blocked

Reported: 2021-04-08 13:19 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-05-26 17:24 UTC (History)
CC List: 2 users (show)
Fixed In Version:
Doc Type: If docs needed, set a value
Doc Text:

```
A flaw was found in PoDoFo 0.9.7. An use-after-
free in PoDoFo::PdfVecObjects::Clear() function
can cause a denial of service via a crafted PDF
file.
```

Clone Of:
Environment:
Last Closed: 2021-04-08 23:35:23 UTC

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

Guilherme de Almeida Suckevicz 2021-04-08 13:19:02 UTC — Description

```
A flaw was found in PoDoFo. An use-after-free in PoDoFo::PdfVecObjects::Clear() function can cause a denial of service via a crafted PDF file.

Reference:
https://sourceforge.net/p/podofo/tickets/129/
```

Guilherme de Almeida Suckevicz 2021-04-08 19:02:09 UTC — Comment 1

```
Created mingw-podofo tracking bugs for this issue:

Affects: fedora-all [ bug 1947636 ]


Created podofo tracking bugs for this issue:

Affects: epel-7 [ bug 1947637 ]
Affects: fedora-all [ bug 1947635 ]
```

Product Security DevOps Team 2021-04-08 23:35:23 UTC — Comment 2

```
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.