Bug 1967014 (CVE-2021-23165) - CVE-2021-23165 htmldoc: heap-buffer-overflow in pspdf_prepare_outpages()

Keywords:	Security ×	**Reported:**	2021-06-02 10:48 UTC by Dhananjay Arunesh
		Modified:	2022-03-19 05:19 UTC (History)
Status:	CLOSED UPSTREAM	**CC List:**	5 users (show)
Alias:	CVE-2021-23165	**Fixed In Version:**	
Product:	Security Response	**Doc Type:**	If docs needed, set a value
Component:	vulnerability	**Doc Text:**	
		Clone Of:	
		Environment:	
Version:	unspecified	**Last Closed:**	2021-06-02 11:32:12 UTC
Hardware:	All		
OS:	Linux		
Priority:	high		
Severity:	high		
Target Milestone:	---		
Assignee:	Red Hat Product Security		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:	1967017 ~~1967016~~		
Blocks:	🔒 1967015		
TreeView+	depends on / blocked		

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

Dhananjay Arunesh 2021-06-02 10:48:12 UTC Description

```
A flaw was found in htmldoc in v1.9.12. Heap buffer overflow in pspdf_prepare_outpages(), in ps-pdf.cxx may lead to execute arbitrary code and denial of service.

Reference:
https://github.com/michaelrsweet/htmldoc/issues/413

Upstream patch:
https://github.com/michaelrsweet/htmldoc/commit/369b2ea1fd0d0537ba707f20a2f047b6afd2fbdc
```

Dhananjay Arunesh 2021-06-02 10:49:39 UTC Comment 1

Created htmldoc tracking bugs for this issue:

Affects: epel-7 [bug 1967017]
Affects: fedora-all [~~bug 1967016~~]

Product Security DevOps Team 2021-06-02 11:32:12 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.

Gianluca Gabrielli 2021-06-03 13:38:36 UTC Comment 3

This has the same fix of 1967009 (CVE-2021-26252)

Gianluca Gabrielli 2021-06-03 13:58:57 UTC Comment 4

Please discard my previous message. This is a different bug than 1967009 (CVE-2021-26252). Upstream patch [0].

[0] https://github.com/michaelrsweet/htmldoc/commit/6e8a95561988500b5b5ae4861b3b0cbf4fba517f.patch

John Helmert III 2022-03-19 05:19:30 UTC Comment 5

Why did it take so long for CVE-2021-23165 (this bug) and CVE-2021-23158 (~~bug 1967010~~) to be released? The bugs were opened in 2021-06 but CVEs were released in 2022-03, 9 months later. This is a big gap for those who depend on on CVEs to know what needs to be patched.

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