Bug 1928437 - There is an illegal WRITE memory access at libcaca/caca/canvas.c:475 (function:caca_resize)in libcaca latest version.

Keywords:		**Reported:**	2021-02-14 01:58 UTC by 245
Status:	CLOSED EOL	**Modified:**	2021-05-25 17:05 UTC (History)
Alias:	None	**CC List:**	3 users (show)
Product:	Fedora	**Fixed In Version:**	
Component:	libcaca	**Doc Type:**	---
		Doc Text:	
Version:	32	**Clone Of:**	
Hardware:	Unspecified	**Environment:**	
OS:	Unspecified	**Last Closed:**	2021-05-25 17:05:41 UTC
Priority:	unspecified	**Type:**	Bug
Severity:	unspecified	**Dependent Products:**	
Target Milestone:	---		
Assignee:	Matthias Saou		
QA Contact:	Fedora Extras Quality Assurance		
Docs Contact:			
URL:			
Whiteboard:			
Depends On:			
Blocks:			

TreeView+ depends on / blocked

Attachments	(Terms of Use)	
The report contains verification steps and POC (4.33 KB, text/plain) 2021-02-14 01:58 UTC, 245	*no flags*	Details
Add an attachment (proposed patch, testcase, etc.)		View All

245 2021-02-14 01:58:52 UTC — Description

```
Created attachment 1756895 [details]
The report contains verification steps and POC

Description of problem:

Use a specific string to call caca_import_canvas_from_memory() the program will crash

Version-Release number of selected component (if applicable):
libcaca - v0.99.beta19

How reproducible:


Steps to Reproduce:
1.Get the source code of libcaca:

2.Compile the libcaca.so library:

$ cd libcaca
$ apt-get install automake libtool pkg-config -y
$ ./bootstrap
$ ./configure
$ make
3.Copy the POC.c & POC_build.sh in /example folder

4.Run POC_build.sh to compile POC.c

5Run POC

Actual results:
=================================================================
==20599==ERROR: AddressSanitizer: SEGV on unknown address 0x601f1009f400 (pc 0x7fd5a381ff76 bp 0x7ffdb2f550d0 sp 0x7ffdb2f54e40 T0)
==20599==The signal is caused by a WRITE memory access.
#0 0x7fd5a381ff75 in caca_resize /work/libcaca/caca/canvas.c:475:47
#1 0x7fd5a384fdc3 in _import_ansi /work/libcaca/caca/codec/text.c:451:17
#2 0x4f921c in main /work/libcaca/examples/POC.c:43:6
#3 0x7fd5a34840b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#4 0x41e34d in _start (/work/libcaca/examples/POC+0x41e34d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /work/2_libfuzzer_Assignment/question3/libcaca/caca/canvas.c:475:47 in caca_resize
==20599==ABORTING


Expected results:


Additional info:
```

245 2021-02-14 02:08:52 UTC — Comment 1

```
Reported to upstream https://github.com/cacalabs/libcaca/issues/52
```

Fedora Program Management 2021-04-29 16:46:08 UTC — Comment 2

```
This message is a reminder that Fedora 32 is nearing its end of life.
Fedora will stop maintaining and issuing updates for Fedora 32 on 2021-05-25.
It is Fedora's policy to close all bug reports from releases that are no longer
maintained. At that time this bug will be closed as EOL if it remains open with a
Fedora 'version' of '32'.

Package Maintainer: If you wish for this bug to remain open because you
plan to fix it in a currently maintained version, simply change the 'version'
to a later Fedora version.

Thank you for reporting this issue and we are sorry that we were not
able to fix it before Fedora 32 is end of life. If you would still like
to see this bug fixed and are able to reproduce it against a later version
of Fedora, you are encouraged  change the 'version' to a later Fedora
version prior this bug is closed as described in the policy above.

Although we aim to fix as many bugs as possible during every release's
lifetime, sometimes those efforts are overtaken by events. Often a
more recent Fedora release includes newer upstream software that fixes
bugs or makes them obsolete.
```

Ben Cotton 2021-05-25 17:05:41 UTC Comment 3

Fedora 32 changed to end-of-life (EOL) status on 2021-05-25. Fedora 32 is no longer maintained, which means that it will not receive any further security or bug fix updates. As a result we are closing this bug.

If you can reproduce this bug against a currently maintained version of Fedora please feel free to reopen this bug against that version. If you are unable to reopen this bug, please file a new report against the current release. If you experience problems, please add a comment to this bug.

Thank you for reporting this bug and we are sorry it could not be fixed.