


```
#12 0x7fdb24c9edd5 in _pixman_image_for_pattern /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/sr
#13 0x7fdb24ca678b in _composite_boxes /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/src/cairo-i
#14 0x7fdb24ca678b in _clip_and_composite_boxes /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/sr
#15 0x7fdb24c953b4 in _cairo_image_surface_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/s
#16 0x7fdb24d0effe in _cairo_surface_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/src/cai
#17 0x7fdb24c1cafd in _cairo_surface_wrapper_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo
#18 0x7fdb24ce55ed in _cairo_recording_surface_replay_internal /home/sourc7/git/gecko-dev-asan/gfx
#19 0x7fdb24cfd1cd in _cairo_recording_surface_replay /home/sourc7/git/gecko-dev-asan/gfx/cairo/ca
```

Flags: sec-bounty?



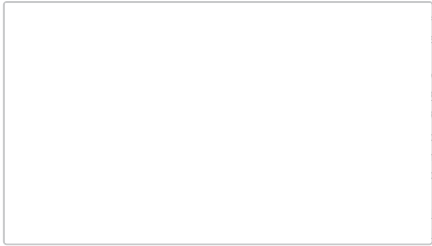
Irvan Kurniawan (:sourc7)

Reporter

Comment 1 • 2 years ago



Attached file [asan-output.txt](#) — [Details](#)



Irvan Kurniawan (:sourc7)

Reporter

Comment 2 • 2 years ago



It turns out that holding down the "enter" key it able to pass the print dialog then Save to PDF, so it straightforward way to trigger the crash.



:Gijs (he/him)

Updated • 2 years ago



Group: firefox-core-security → gfx-core-security

Component: Security → Graphics

Product: Firefox → Core



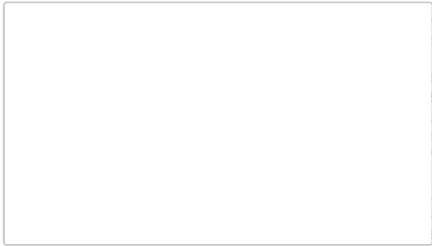
Irvan Kurniawan (:sourc7)

Reporter

Comment 3 • 2 years ago



Attached file [asan-windows.txt](#) — [Details](#)



Andrew McCreight (:mccr8)

Comment 4 • 2 years ago



Those stacks are really deep in Cairo. I tried to look the stacks but I couldn't make much sense of them.

Requiring a save to PDF maybe mitigates it a little bit, but it still sounds bad. It looks like cairo-recording-surface.c was last updated in 2012.

Keywords: [csectype-uaf](#)

Summary: AddressSanitizer: heap-use-after-free [@ _pixman_image_validate] → AddressSanitizer: heap-use-after-free [@ _pixman_image_validate] when saving to PDF



Emilio Cobos Álvarez (:emilio)

Comment 5 • 2 years ago



Jonathan is working on a cairo update atm iirc.



Emilio Cobos Álvarez (:emilio)

Updated • 2 years ago



Status: UNCONFIRMED → NEW

Ever confirmed: true



Andrew McCreight (:mccr8)

Updated • 2 years ago



See Also: → [1606944](#)



Daniel Veditz (:dveditz)

Updated • 2 years ago



Keywords: [sec-moderate](#)



Irvan Kurniawan (:sourc7)

Reporter

Comment 7 • 2 years ago



Update: I can also reproduce this crashes when print destinations other than "Save to PDF" (e.g. Microsoft Print to PDF, Fax, OneNote)



Irvan Kurniawan [:sourc7]

Reporter

Updated • 2 years ago



Summary: AddressSanitizer: heap-use-after-free [@ _pixman_image_validate] when saving to PDF → AddressSanitizer: heap-use-after-free [@ _pixman_image_validate] when print or save to PDF



Jonathan Kew [:jfkthame]

Assignee

Comment 8 • 2 years ago



I can confirm this reproduces in a local ASAN build of mozilla-central; but it does not reproduce with my current patch stack to update to cairo-1.17.4*. So [bug-739096](#) should resolve this.



Andrew McCreight [:mccr8]

Updated • 2 years ago



Whiteboard: [reporter-external] [client-bounty-form] [verif?] → [reporter-external] [client-bounty-form] [verif?][fixed by Cairo update]



Tyson Smith [:tsmith]

Comment 9 • 2 years ago



Looks like this was indeed fixed by [bug-739096](#). It was last found by the fuzzer while fuzzing m-c 20210427-3009bdef939c.

Status: NEW → RESOLVED

Closed: 2 years ago

Resolution: --- → FIXED



Irvan Kurniawan [:sourc7]

Reporter

Comment 10 • 2 years ago



(In reply to Tyson Smith [:tsmith] from [comment #9](#))

Looks like this was indeed fixed by [bug-739096](#). It was last found by the fuzzer while fuzzing m-c 20210427-3009bdef939c.

Thanks Tyson, I also confirmed that I no longer able to reproduce this in Firefox 90.0a1 (2021-05-06) (64-bit).

Status: RESOLVED → VERIFIED



Daniel Veditz [:dveditz]

Updated • 2 years ago



Depends on: [739096](#)

Flags: sec-bounty? → sec-bounty+

Whiteboard: [reporter-external] [client-bounty-form] [verif?][fixed by Cairo update] → [fixed by Cairo update][reporter-external] [client-bounty-form] [verif?]



Ryan VanderMeulen [:RyanVM]

Updated • 2 years ago



Assignee: nobody → jfkthame
Group: gfx-core-security → core-security-release

[status-firefox88](#): --- → wontfix

[status-firefox89](#): --- → wontfix

[status-firefox90](#): --- → fixed

[status-firefox-esr78](#): --- → wontfix

Target Milestone: --- → 90 Branch



Tom Ritter [:tjr]

Updated • 2 years ago



Whiteboard: [fixed by Cairo update][reporter-external] [client-bounty-form] [verif?] → [fixed by Cairo update][reporter-external] [client-bounty-form] [verif?][adv-main90+]

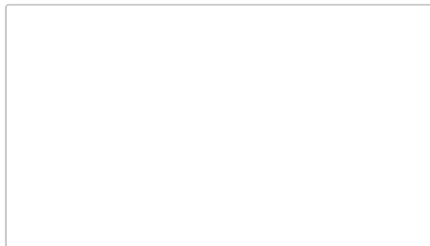


Tom Ritter [:tjr]

Comment 11 • 2 years ago



Attached file [advisory.txt](#) — Details



Tom Ritter [:tjr]

Updated • 2 years ago



Alias: CVE-2021-29972



Daniel Veditz [:dveditz]

Updated • 1 year ago



Group: ~~core-security-release~~

You need to [log in](#) before you can comment on or make changes to this bug.