Copy Summary ▾ View ▾

Closed Bug 1696816 (CVE-2021-29972) Opened 2 years ago Closed 2 years ago

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

▾ Categories

Product: Core ▾
Component: Graphics ▾
Type: task
Priority: Not set Severity: --

▾ Tracking

Status: VERIFIED FIXED
Milestone: 90 Branch

Tracking Flags:

	Tracking	Status
firefox-esr78	---	wontfix
firefox88	---	wontfix
firefox89	---	wontfix
firefox90	---	fixed

▸ People (Reporter: sourc7, Assigned: jfkthame)

▸ References

▸ Details (Keywords: csectype-uaf, sec-moderate, Whiteboard: [fixed by Cairo update][reporter-external] [client-bounty-form] [verif?][adv-main90+])

▾ Attachments

testcase.html Details
2 years ago **Irvan Kurniawan (:sourc7)**
197 bytes, text/html

asan-output.txt Details
2 years ago **Irvan Kurniawan (:sourc7)**
24.38 KB, text/plain

asan-windows.txt Details
2 years ago **Irvan Kurniawan (:sourc7)**
19.95 KB, text/plain

advisory.txt Details
2 years ago **Tom Ritter [:tjr]**
297 bytes, text/plain

Bottom ↓ Tags ▾ Timeline ▾

Irvan Kurniawan (:sourc7) Reporter
Description • 2 years ago

*Attached file **testcase.html** — Details*

By set CSS universal selector `*` with property `clip-path: polygon` `<clip-source>` and `<basic-shape>` with value more than or equal to 13 then add `mix-blend-mode: soft-light` to the selector. After print the web pages dialog show then Save to PDF, the entire browser is crashed with heap-use-after-free.

Affected version:

- Firefox Nightly 88.0a1 (2021-03-07) (64-bit) on Arch Linux and Windows 10
- Firefox Release 86.0 (64-bit)
- Firefox ESR 78.8.0esr (64-bit)

Steps to reproduce:

1. Visit attached testcase.html
2. When print dialog show, select Destination "Save to PDF" (default on my desktop) or "Print to File" (on Firefox ESR Linux)
3. Click "Save" or "Print"
4. Browser crashed

ASAN output:

```
=================================================================
==551946==ERROR: AddressSanitizer: heap-use-after-free on address 0x612004964470 at pc 0x7fdb24e356a1
READ of size 4 at 0x612004964470 thread T0
    #0 0x7fdb24e356a0 in _pixman_image_validate /home/sourc7/git/gecko-dev-asan/gfx/cairo/libpixman/sr
    #1 0x7fdb24eac48f in _moz_pixman_image_composite32 /home/sourc7/git/gecko-dev-asan/gfx/cairo/libpi
    #2 0x7fdb24ca6a43 in _composite_boxes /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/src/cairo-im
    #3 0x7fdb24ca6a43 in _clip_and_composite_boxes /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/src
    #4 0x7fdb24c953b4 in _cairo_image_surface_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/sr
    #5 0x7fdb24d0effe in _cairo_surface_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/src/cair
    #6 0x7fdb24c1cafd in _cairo_surface_wrapper_paint /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/
    #7 0x7fdb24ce55ed in _cairo_recording_surface_replay_internal /home/sourc7/git/gecko-dev-asan/gfx/
    #8 0x7fdb24cfd1cd in _cairo_recording_surface_replay /home/sourc7/git/gecko-dev-asan/gfx/cairo/cai
    #9 0x7fdb24cfd1cd in _cairo_recording_surface_acquire_source_image /home/sourc7/git/gecko-dev-asan
    #10 0x7fdb24d0e8fd in _cairo_surface_acquire_source_image /home/sourc7/git/gecko-dev-asan/gfx/cair
    #11 0x7fdb24c9edd5 in _pixman_image_for_surface /home/sourc7/git/gecko-dev-asan/gfx/cairo/cairo/sr
```

```
    #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: → ~~1696844~~

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 739896~~ 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 739896~~. 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 739896~~. 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: ~~739896~~
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.

Top ↑