☆ Starred by 5 users

Owner:	thomasanderson@chromium.org
CC:	a...@chromium.org huangdarwin@chromium.org dvadym@chromium.org msi...@igalia.com pbos@chromium.org harrisjay@chromium.org adetaylor@chromium.org ajgo@google.com weili@chromium.org nickdiego@igalia.com tbergquist@chromium.org bsep@chromium.org lazyboy@chromium.org jdonnelly@chromium.org cyan@chromium.org robliao@chromium.org kylixrd@chromium.org tapted@chromium.org msw@chromium.org thomasanderson@chromium.org corising@chromium.org connily@chromium.org ellyj...@chromium.org vasi...@chromium.org leecraso@gmail.com jdoer...@chromium.org pkasting@chromium.org erikc...@chromium.org dcheng@chromium.org sky@chromium.org pwnall@chromium.org est...@chromium.org osh...@chromium.org dfried@chromium.org adun...@igalia.com mamir@chromium.org achuith@chromium.org there...@gmail.com fhorschig@chromium.org
Status:	Verified *(Closed)*
Components:	Blink>DataTransfer
Modified:	Apr 28, 2021
Backlog-Rank:	----

Issue 1138143: segmentation fault in mojom::clipboard

Reported by work3...@gmail.com on Wed, Oct 14, 2020, 4:34 AM EDT

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36

Steps to reproduce the problem:
chromium: 88.0.4293.0
1. Download and extract asan-linux-release-816894.zip from (https://www.googleapis.com/download/storage/v1/b/chromium-browser-asan/o/linux-release%2Fasan-linux-release-816894.zip?generation=1602654017334593&alt=media)
2. cp /path/to/poc.html /path/to/asan-linux-release-816894
3. python3 -m http.server 8090
4. ./chrome --enable-blink-features=MojoJS http://localhost:8090/poc.html

What is the expected behavior?
The result of readText () should be displayed on the console(devtool).

What went wrong?
segmentation fault

Did this work before? N/A

Chrome version: 88.0.4293.0 Channel: canary
OS Version: Ubuntu 18.04 LTS
Flash Version:

Sorry, the following issue is mistake.
https://bugs.chromium.org/p/chromium/issues/detail?id=1138141

poc.html
950 bytes View Download

crash.log
15.2 KB View Download

Comment 1 by ClusterFuzz on Wed, Oct 14, 2020, 3:14 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5632575442059264.

Comment 2 by palmer@chromium.org on Thu, Oct 15, 2020, 5:13 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: huangdarwin@chromium.org
Cc: dcheng@chromium.org
Labels: Security_Impact-Head
Components: Blink

huangdarwin, could you please take a look? Thanks!

Comment 3 by huangdarwin@chromium.org on Thu, Oct 15, 2020, 6:30 PM EDT

I tried to repro using given instructions (as well as building an asan build locally, and symbolizing via valgrind instructions[1]). Through both approaches, I wasn't able to correctly symbolize and see function calls in stack traces, though it did reliably crash, and did fail to crash if I disabled MojoJS.

Instead, I saw could once see a crash from a blink FontCache CHECK[2] failing. Other times, I'd see crashes with various LOG(ERROR) logs, often with something related to fonts. I wonder if this is some interesting interaction between clipboard and fonts?

work38thaxus@, do you know if you can see the call stack for the crash? Or how what I can do to see this myself? Thanks!

[1]: https://chromium.googlesource.com/chromium/src/+/HEAD/docs/asan.md
[2]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/fonts/font_cache.cc;l=472;drc=8c74b580dbc84f465311d00b853b9f944e64737b

Comment 4 by huangdarwin@chromium.org on Thu, Oct 15, 2020, 6:40 PM EDT

For reference, in case it helps, my GN args were the following:

```
use_goma = true
is_asan = true
is_debug = false  # Release build
enable_full_stack_frames_for_profiling = true
```

Comment 5 by tkent@chromium.org on Thu, Oct 15, 2020, 8:52 PM EDT

Components: -Blink Blink>DataTransfer

Comment 6 by work3...@gmail.com on Sun, Oct 18, 2020, 11:35 PM EDT

Hi.

I used ASAN build, but I also could not able to correctly symbolize and see function calls in stack traces. (I could not see ASAN report correctly)

In my opinion, sometimes after executing ui::Clipboard X11::X11 Details::WaitAndGetTargetsList(ui::Clipboard Buffer), the value of rsp becomes invalid, and subsequent function calls may fail.
Maybe this caused ASAN to not work properly.

I attached updated poc(during verification) and gdb log.

memo.log
4.1 KB View Download

poc.html
1.6 KB View Download

Comment 7 by huangdarwin@chromium.org on Mon, Oct 19, 2020, 9:10 PM EDT

Thank you, work38thaxus@. The memo.log is very interesting... I suspect some issue with re-entrancy regarding ui::Clipboard X11::X11 Details::WaitAndGetTargetsList(ui::Clipboard Buffer)... I recall seeing bugs[1][2][3] and crashes like that in the past, where the X11 message loop would have some sort of issue that led to crashes...

dcheng@, sorry, do you know how we could try to fix this potential re-entrancy crash? I don't have any experience with diagnosing/fixing these issues yet.

[1]: https://crbug.com/748441#c2
[2]: ~~https://crbug.com/932955#c8~~
[3]: https://crbug.com/931874

Comment 8 by sheriffbot on Fri, Oct 30, 2020, 6:45 PM EDT

Labels: reward-potential

Comment 9 by kenrb@chromium.org on Mon, Nov 9, 2020, 5:15 PM EST

Labels: Security_Severity-High Pri-1

dcheng@ are you able to respond to comment 7?

Also we don't have a severity set on this bug yet, but I'm going to assume for now that is is exploitable and should be a Severity-High (otherwise it isn't a security bug at all).

Comment 10 by sheriffbot on Tue, Nov 10, 2020, 12:21 PM EST

huangdarwin: Uh oh! This issue still open and hasn't been updated in the last 21 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 11 by sheriffbot on Tue, Nov 10, 2020, 12:53 PM EST

Labels: Target-88 M-88

Setting milestone and target because of Security_Impact=Head and high severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 12 by sheriffbot on Tue, Nov 10, 2020, 1:19 PM EST

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 13 by huangdarwin@chromium.org on Tue, Nov 10, 2020, 5:30 PM EST

Daniel, per comment 7, sorry, do you know how to approach re-entrancy crashes for the clipboard?

Actually, I don't think that a segfault is usually classified as a security bug, since I'm not sure how this could be exploited to achieve remote code execution or view extra resources (though this certainly should be a stability bug). Does this sound right? If so, we should remove the ReleaseBlock-Stable and Security_Severity tags.

Comment 14 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 3:49 PM EST

Cc: pwnall@chromium.org

Comment 15 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 4:05 PM EST

To give a bit more information, the issue here seems to be that, when quickly/repeatedly calling[1] the mojo ClipboardHost's readText function[2], we hit a re-entrancy segfault crash somewhere in ui::Clipboard X11::X11 Details::WaitAndGetTargetsList(ui::Clipboard Buffer)[3], possibly from multiple instances calling this at once.

[1]: See poc.html in description
[2]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/public/mojom/clipboard/clipboard.mojom;l=47;drc=c73e50a7cd345da7ee33ebda32acfcc8f0b26dc5
[3]: https://source.chromium.org/chromium/chromium/src/+/master:ui/base/clipboard/clipboard_x11.cc;l=354;drc=281086aeca412de952c180411560c7ca68a5b97b

Comment 16 by pwnall@chromium.org on Wed, Nov 11, 2020, 4:06 PM EST

#13: "Segmentation fault" (SIGSEGV) is an unhelpful x86 term for invalid memory access.

Invalid memory accesses are generally security issues. They suggest that we're setting some pointer to an incorrect value, so the code setting the pointer isn't working as intended. This opens up the possibility that an attacker may be able to get control of the pointer's value, and cause memory accesses to a controlled address.

If we're sure the Clipboard code around the impacted area hasn't changed in a long time, this doesn't need to be release-blocking. Before clearing that flag, let's make sure we vetted any recent changes.

If we're sure the bug is entirely within X11 and we're not misusing the API in any way, then we can consider removing the Security labels.

Comment 17 by pwnall@chromium.org on Wed, Nov 11, 2020, 4:08 PM EST

#15: Would it make sense to build a queue for the mojo calls?

Possible strategies:

1) While the underlying platform call executes, all incoming Read*() callbacks are queued. When the platform call completes, all callbacks are invoked with the same result.
2) Read*() calls are queued and executed in order.
3) Incoming Read*() calls are dropped while an underlying platform call is already underway.

Comment 18 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 4:47 PM EST

Labels: -ReleaseBlock-Stable

Re: Comment 16: Oops, thanks for the clarification around segfaults and security.

I don't think clipboard threading/calls have been changed much, and vetted recent changes to confirm this. Recent (last 9 months) changes around this codepath (mojo readText -> x11's WaitAndGetTargetsList) mostly just involve refactoring of: X11 atoms[1], DLP[2][3][4]. Changes that make functional changes but shouldn't affect threading include x11 selection checks[5], or adding metrics for clipboard writes[6].

I'm sure the bug is entirely within X11, but I'm not sure that we're not misusing the API (though if we are, I suspect it has been this way for a while). Therefore, I'll leave the security label there for now.

[1]: https://crrev.com/c/2202789 [XProto] Replace XAtom with x11::Atom
[2]: https://crrev.com/c/2489889 DLP: Rename ClipboardDataEndpoint and ClipboardDlpController
[3]: https://crrev.com/c/2266901 Pass destination on clipboard read
[4]: https://crrev.com/c/2346288 Change Clipboard::Read*() refs to set dst
[5]: https://crrev.com/c/2242747 [XProto] Fix hang during paste with XWayland
[6]: https://crrev.com/c/2255741 ui/base/clipboard: Add logging for read and write of various formats.

Comment 19 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 4:48 PM EST

Labels: ReleaseBlock-NA

Comment 20 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 5:20 PM EST

Cc: thomasanderson@chromium.org

I did some digging on related issues and found ~~Issue 839250~~, which has an almost identical repro case (that bug's repro calls readText() many times, then writeText() once).

also, +cc:thomasanderson@ for linux expertise.

Comment 21 by huangdarwin@chromium.org on Wed, Nov 11, 2020, 6:53 PM EST

work38thaxus@, could you please try symbolizing the stack using asan_symbolize.py? Something like `./chrome --enable-blink-features=MojoJS http://localhost:8090/poc.html 2>&1 | tools/valgrind/asan/asan_symbolize.py` to replace the last step of the description's repro. I'm still not able to repro the clipboard-related segfault

Comment 22 by dcheng@chromium.org on Wed, Nov 11, 2020, 7:53 PM EST

First, sorry for missing the pings earlier! I totally missed the emails for this :(

As for the bug here, the original issue was a use-after-free: we could reentrantly call the Read* methods--and since ClipboardHostImpl itself was owned by a StrongBinding, once we closed the message pipe from the renderer, the implementation itself would get deleted. This is, of course, problematic when we have reentrant Mojo IPC calls to ClipboardHostImpl::Read* on the stack. We fixed it by cleaning up the ClipboardHostImpl with a non-nestable task, so in theory, we shouldn't have that bug anymore.

I don't think that's the bug here: while the stack is (unfortunately) not symbolized, ASan is generally pretty good about diagnosing memory safety errors in instrumented code...

It, of course, does not stop this from being a UAF in other code that gets confused by the reentrancy. We should try to narrow down where this crash is coming from. One thing we could try is testing with MSan, which does have instrumented system libraries. Unfortunately, running with MSan is also much more annoying...

As for potential fixes, a long time ago, I requested that we add RunWithTimeout to RunLoop. The only reason we run a nested RunLoop is to be able to timeout the wait if it takes too long. Unfortunately, RunWithTimeout was reverted since it wasn't used much and the tests were flaky:
https://source.chromium.org/chromium/chromium/src/+/cfde7b381975b4ce50338f97a7ed0547a9ab6fa3

However, we could try relanding it and seeing if that helps alleviate this particular crash.

Comment 23 by dcheng@chromium.org on Wed, Nov 11, 2020, 8:11 PM EST

Btw, we might want to see if StartDragging is similarly problematic--though it's simpler to fix there, since we can simply disallow nested StartDragging invocations. I don't see any guard there today, so I wouldn't be surprised if there were problems there too...

Comment 24 by work3...@gmail.com on Fri, Nov 13, 2020, 7:30 AM EST

huangdarwin@
I've built chrome with asan locally and tried `./chrome --enable-blink-features=MojoJS http://localhost:8090/poc.html 2>&1 | tools/valgrind/asan/asan_symbolize.py`.
I attach some logs of the above command execution results. also, I noticed from this log that there are no clipboard related symbols. (sorry for misleading title)

symbolize.log
15.4 KB View Download

symbolize2.log
66.9 KB View Download

Comment 25 by huangdarwin@chromium.org on Fri, Nov 13, 2020, 3:18 PM EST

Thanks for the replies and context, dcheng@. I did try "quickly" setting up msan and found it annoying as well... :P

Hmm attempting either a RunWithTimeout per comment 22, or some sort of mojo queue per comment 17 both sound like viable solutions, though I'd hesitate to do that until we can verify the clipboard segfault, since those wouldn't be tiny/"trivial" changes. Also fwiw, if clipboard has this segfault, I agree suspect that drag-and-drop might as well.

Comment 26 by huangdarwin@chromium.org on Fri, Nov 13, 2020, 3:29 PM EST

Thank you for the logs, work38thaxus@.

The first "symbolize.log" file shows a Skia SIGSEGV[1]. I'm personally not able to reproduce this.

The second "symbolize2.log" file shows the blink FontCache CHECK I encountered in Comment 3.

It seems this segfault might not be easily reproducible. I'm not sure if this is due to different BUILD parameters between local asan builds and the asan build you were using in comment 6, or if this is simply difficult to reproduce or fixed already. work38thaxus@, sorry for the repeated questions, but how did you repro in comment 6 to get that log, and how did that differ from how you repro'ed in comment 24? I'm able to get approximately the logs you have in Comment 24, but not the logs you had in comment 6.

[1]:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/skia/src/gpu/ops/GrTextureOp.cpp;l=931;drc=e25c30034a633d873a00d89cee4451545941a7ef

Comment 27 by huangdarwin@chromium.org on Fri, Nov 13, 2020, 3:30 PM EST

(I am also aware of flaky crashes / sigsegv's / CHECKs happening on ToT builds sometimes, so I believe the Skia SIGSEGV exists, but just noting that I didn't repro it myself)

Comment 28 by huangdarwin@chromium.org on Fri, Nov 13, 2020, 6:22 PM EST

I tried modifying the repro and can confirm that the fontcache CHECK is only hit when we spam many readText calls, so I suspect maybe there isn't a reproducible clipboard segfault (pending comment 26), but rather that clipboard readText calls can saturate the browser on navigation, so that fontcache doesn't have time to startup and hits the CHECK.

Comment 29 by work3...@gmail.com on Sat, Nov 14, 2020, 8:09 AM EST

huangdarwin@
I tried to reproduce crash of comment 6. but I couldn't confirm exactly the same log.
I attach some logs during the retry.

Below are my steps:
1. gdb -q chrome
2. set follow-folk-mode parent
3. r --enable-blink-features=MojoJS http://localhost:8090/poc.html

retry02.log
5.9 KB View Download

retry01.log
5.1 KB View Download

Comment 30 by sheriffbot on Wed, Nov 18, 2020, 12:21 PM EST

Labels: -Security_Impact-Head Security_Impact-Beta

Comment 31 by sheriffbot on Sat, Nov 28, 2020, 12:21 PM EST

huangdarwin: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 32 by huangdarwin@chromium.org on Wed, Dec 2, 2020, 10:15 PM EST

Thanks for providing the logs, work38thaxus@! And sorry I forgot to reply earlier. It seems in retry01.log, the segfault is occuring when ReadText gets stuck sometime in WaitAndGetTargetsList, when syncing with the X server. The deepest we can see is a call[1] to xcb_wait_for_reply(). In retry02.log, we somehow get stuck in ClipboardX11::DispatchXEvent, after which we again get into X code and hit the breakpoint.

Comment 33 by huangdarwin@chromium.org on Wed, Dec 2, 2020, 10:22 PM EST

It still seems difficult to get a reliable repro. That said, my understanding is that sending multiple clipboard reads in quick succession can hit us with some re-entrancy issues in X code, which likely isn't meant to handle re-entrancy. It may also block the browser process a bit, so that "some things" don't set up correctly, hence the unrelated Fontcache CHECKs being hit.

I suspect that the right fix for this may be to avoid allowing multiple clipboard reads to be initiated, or at least nested+running, at the same time. We could do this in one of 2 ways:
(1) As suggested by dcheng@ in Comment 22, reverting the RunWithTimeout removal and seeing if that helps. This notably should only affect ui/base/x/ code, so would be a precise change that won't affect other platforms.
(2) As suggested by pwnall@ in Comment 17, I believe building a queue could definitely be a viable way to fix this as well. If we did this on top of a X RunLoop, we'd probably want to do this in the ClipboardHostImpl layer. I'm not sure if this would be redundant with the X RunLoop that we already have though, and while it could protect us from similar issues on other platforms (Windows/Mac/Android/etc), I think X11 really is the only platform that experiences this issue.

(Also oops, this[1] was meant to be the "[1]" link in Comment 32.)
[1]: https://source.chromium.org/chromium/chromium/src/+/master:ui/gfx/x/xproto_types.cc;l=133;drc=d81c5852498699fe3cd812e78d31c77c28e29281

Comment 34 by huangdarwin@chromium.org on Wed, Dec 2, 2020, 10:25 PM EST

Labels: -Security_Severity-High Security_Severity-Medium Pri-2

I suspect this issue could be considered a lower severity (low/medium?), since this is generally hitting a fontcache check/crash, at least in my testing. It does also seem a bit more complex to fix/test/verify, due the difficulty of getting similar repeatable traces. Therefore, I'll lower the severity/priority. Please let me know if this doesn't sound right though, dcheng@.

Comment 35 by thomasanderson@chromium.org on Thu, Dec 3, 2020, 1:25 PM EST

Cc: adun...@igalia.com

+adunaev for X11 clipboard (stack traces are in c#29)

Comment 36 by sheriffbot on Thu, Dec 3, 2020, 1:40 PM EST

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 37 by huangdarwin@chromium.org on Thu, Dec 3, 2020, 8:23 PM EST

Status: Available (was: Assigned)
Owner: ----
Cc: huangdarwin@chromium.org
Labels: Pri-2

(I'll be prioritizing some other higher-pri stuff for now, so please feel free to take this bug)

Comment 38 by adun...@igalia.com on Fri, Dec 4, 2020, 12:52 AM EST

Cc: msi...@igalia.com nickdiego@igalia.com

Thank you for pulling me in.

+msisov, +nickdiego for X11.

Comment 39 by ajgo@google.com on Wed, Dec 23, 2020, 7:39 PM EST

sheriff: could someone be the owner of this security bug?

Comment 40 by adetaylor@google.com on Thu, Jan 7, 2021, 12:56 PM EST

Status: Assigned (was: Available)
Owner: huangdarwin@chromium.org
Labels: -ReleaseBlock-NA -Security_Severity-Medium -Security_Impact-Beta Security_Impact-Stable Security_Severity-High Pri-1

huangdarwin@, sorry, security issues can't remain Available, so I've got to dump this back on you.

I'm afraid I need to question some of the labels here too:

Security_Impact - all the discussion suggests that this is a long-standing issue which almost certainly affects stable (M87) so I am fixing Security_Impact to be Stable.
ReleaseBlock - Sheriffbot wanted to block release because it thought this was a regression, due to the wrong Security_Impact label. It sounds like it isn't a recent regression so there should be no need to block any releases.
Security_Severity - I'm afraid I'm not comfortable with #c34. This is a browser process crash, so is at the upper end of 'high' severity as a relatively rare sandbox escape. I understand from your comment that it's generally hitting a CHECK, which is not a security concern, but from #c29 there does seem to be a remaining legitimate memory safety issue. If an attacker can find a way to exploit that reliably, they have a sandbox escape. I think we have to assume this remains high priority.
Pri - whether it's Security_Severity high or medium, it's still Pri-1.

Next steps:
To gather additional information, I think we should try to persuade ClusterFuzz to try to reproduce this, per https://chromium.googlesource.com/chromium/src/+/master/docs/security/clusterfuzz-for-sheriffs.md#MojoJS. If it succeeds (*if*) we'll get all the symbolized stack traces we need. I suspect it'll be flakey or unreproducible though. I may not get around to this imminently, but I'll add it to my to-do list. Apart from that I agree with the plans in #c33 to avoid assuming re-entrancy in these APIs.

Comment 41 by thomasanderson@chromium.org on Thu, Jan 7, 2021, 1:03 PM EST

For the record, this is just one of many X11 clipboard related UAF issues:
~~https://crbug.com/1161143~~ LocationBar
~~https://crbug.com/1161144~~ bookmark openall
~~https://crbug.com/1161145~~ omniboxfield
~~https://crbug.com/1161146~~ TextField/FocusManager
~~https://crbug.com/1161147~~ Password paste
~~https://crbug.com/1161149~~ OmniboxMenu
~~https://crbug.com/1161151~~ NewTabButtonPressed
~~https://crbug.com/1161152~~ bookmarksmenu

Long term, the best fix is to make the clipboard APIs async:
https://crbug.com/443355

Comment 42 by huangdarwin@chromium.org on Fri, Jan 8, 2021, 6:53 AM EST

Owner: pwnall@chromium.org

Re Comment 40: Fair, it does make sense that there is a legitimate memory safety issue somewhere here. It is difficult for us to reliably reproduce for now (per #c34), but could be quite bad if an attacker can reliably reproduce/use it. I'm still unsure that this should be my top priority now, so I'll assign to pwnall@ for prioritization (Incidentally, I'll also be OOO for 2 weeks soon so won't be able to respond in a timely manner).

Re Comment 41: Wow, there's more X11 Clipboard UaFs here than I was previously aware of...

Comment 43 by huangdarwin@chromium.org on Fri, Jan 8, 2021, 7:03 AM EST

(oops, accidentally submitted #c42 prematurely)

Re Comment 41: Agreed that the best long-term fix is to make clipboard APIs async. The comments in Issue 443355 suggest that this hasn't been done yet due to it being a deeply complex task, but prioritization might change if there's a large class of UaFs caused by this? In the meantime, suggested fixes in #c33 do seem like easier short-term fixes (than making clipboard async), for this specific bug.

Comment 44 by sheriffbot on Fri, Jan 8, 2021, 2:04 PM EST

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 45 by adun...@igalia.com on Mon, Jan 11, 2021, 3:27 AM EST

FTR, as an update to c41: add ~~issue 1161141~~ (UAF in ContextMenu) to the list.

Comment 46 by ClusterFuzz on Mon, Jan 11, 2021, 1:59 PM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5673785771753472.

Comment 47 by ClusterFuzz on Mon, Jan 11, 2021, 3:38 PM EST

Labels: OS-Windows

Comment 48 by ClusterFuzz on Mon, Jan 11, 2021, 3:44 PM EST

Labels: Unreproducible

ClusterFuzz testcase 5673785771753472 appears to be flaky, updating reproducibility label.

Comment 49 by bugdroid on Fri, Jan 15, 2021, 8:00 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f6658bc4fcfe269c53f8806e02492c658bedb09f

commit f6658bc4fcfe269c53f8806e02492c658bedb09f
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Sat Jan 16 00:59:21 2021

Avoid spinning a nested message loop for X11 clipboard

BUG=443355,~~1138143~~,~~1161141~~,~~1161143~~,~~1161144~~,~~1161145~~,~~1161146~~,~~1161147~~,~~1161149~~,~~1161151~~,~~1161152~~

Change-Id: I5c95a9d066683d18f344d694e517274e3ef7ccb4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2622521
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/heads/master@{#844318}

[modify] https://crrev.com/f6658bc4fcfe269c53f8806e02492c658bedb09f/ui/base/x/selection_requestor_unittest.cc
[modify] https://crrev.com/f6658bc4fcfe269c53f8806e02492c658bedb09f/ui/base/x/selection_requestor.cc

Comment 50 by thomasanderson@chromium.org on Fri, Jan 15, 2021, 8:12 PM EST
Status: Fixed (was: Assigned)

Comment 51 by sheriffbot on Sat, Jan 16, 2021, 1:56 PM EST
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 52 by sheriffbot on Sat, Jan 16, 2021, 2:21 PM EST
Labels: Merge-Request-88

Requesting merge to beta M88 because latest trunk commit (844318) appears to be after beta branch point (827102).

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 53 by sheriffbot on Sat, Jan 16, 2021, 2:24 PM EST
Labels: -Merge-Request-88 Merge-Review-88 Hotlist-Merge-Review

This bug requires manual review: We are only 2 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: govind@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), srinivassista @(Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 54 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST
Labels: -reward-potential external_security_report

Comment 55 by sheriffbot on Thu, Jan 21, 2021, 12:43 PM EST
Labels: reward-topanel

Comment 56 by ClusterFuzz on Fri, Jan 22, 2021, 8:23 PM EST
Labels: Needs-Feedback

ClusterFuzz testcase 5673785771753472 is still reproducing on tip-of-tree build (trunk).

Please re-test your fix against this testcase and if the fix was incorrect or incomplete, please re-open the bug. Otherwise, ignore this notification and add the ClusterFuzz-Wrong label.

Comment 57 by pwnall@chromium.org on Fri, Jan 22, 2021, 9:49 PM EST
Owner: thomasanderson@chromium.org
Cc: -thomasanderson@chromium.org

thomasanderson@: Thank you for fixing this!

Comment 58 by ClusterFuzz on Sun, Jan 24, 2021, 7:02 PM EST
Status: Verified (was: Fixed)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5673785771753472 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mojo&range=844293:844296

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 59 by adetaylor@google.com on Tue, Jan 26, 2021, 4:54 PM EST
Labels: Merge-Request-89

Looks to have landed after M89 branch point so adding merge request.

Comment 60 by adetaylor@google.com on Tue, Jan 26, 2021, 7:53 PM EST
Labels: -Merge-Request-89 Merge-Approved-89

I'm going to use this bug to handle merge requests for the squillions of bugs in the CL in #c49.

Approving merge to M89, branch 4389.

I suspect I'll approve merge to M88 on Thursday before our next security refresh if no problems have appeared by then.

Comment 61 by adetaylor@google.com on Wed, Jan 27, 2021, 12:53 PM EST
Labels: -Merge-Review-88 Merge-Approved-88

Also approving merge to M88, branch 4324, unless any problems have shown up in Canary or similar. Please merge.

Comment 62 by thomasanderson@chromium.org on Wed, Jan 27, 2021, 5:31 PM EST
The merge will also require a dependency CL:
https://chromium.googlesource.com/chromium/src/+/f392e62ff77b1de000421de1da66ef7c016056af
Is it ok to merge that too?

Comment 63 Deleted

Comment 64 by adetaylor@google.com on Wed, Jan 27, 2021, 6:12 PM EST

Labels: -Merge-Approved-88 -Merge-Approved-89 Merge-Review-88 Merge-Review-89

Actually... merge approval to both M88 and M89 temporarily rescinded.

This is Linux-only, so has not been functional in a Canary build yet. And due to a quirk of the release cycle, no dev build has been made with this change yet. We'll have to wait until this has baked a little in dev before merging to stable. Dev build should go out tomorrow.

Comment 65 by adetaylor@google.com on Wed, Jan 27, 2021, 6:13 PM EST

Labels: -OS-Windows

Comment 66 by adetaylor@google.com on Wed, Jan 27, 2021, 7:07 PM EST

Cc: kolos@chromium.org tbergquist@chromium.org ellyj...@chromium.org sky@chromium.org bsep@chromium.org achuith@chromium.org collinbaker@chromium.org a...@chromium.org kylixrd@chromium.org cyan@chromium.org lazyboy@chromium.org adetaylor@chromium.org ajgo@google.com osh...@chromium.org vasi...@chromium.org jdoer...@chromium.org fhorschig@chromium.org dvadym@chromium.org robliao@chromium.org corising@chromium.org est...@chromium.org tapted@chromium.org pbos@chromium.org harrisjay@chromium.org jdonnelly@chromium.org pkasting@chromium.org msw@chromium.org connily@chromium.org dfried@chromium.org mamir@chromium.org thomasanderson@chromium.org erikc...@chromium.org weili@chromium.org

~~Issue 1161141~~ has been merged into this issue.
~~Issue 1161143~~ has been merged into this issue.
~~Issue 1161146~~ has been merged into this issue.
~~Issue 1161147~~ has been merged into this issue.
~~Issue 1161151~~ has been merged into this issue.
~~Issue 1161152~~ has been merged into this issue.

Comment 67 by thomasanderson@chromium.org on Wed, Jan 27, 2021, 8:09 PM EST

~~Issue 1161149~~ has been merged into this issue.

Comment 68 by thomasanderson@chromium.org on Wed, Jan 27, 2021, 8:10 PM EST

~~Issue 1161145~~ has been merged into this issue.

Comment 69 by adetaylor@chromium.org on Fri, Jan 29, 2021, 3:40 PM EST

Cc: leecraso@gmail.com

Comment 70 by leecraso@gmail.com on Sun, Jan 31, 2021, 10:44 PM EST

Thanks for the cc. According to the debugging information of comment 29, I think the root cause of the issue is: frequent calling of |readText()| to create nested loops leads to constant push on the stack and eventually OOB access to space above the stack.

```
                        <----- 0x7fffff7fef90 OOB!
-----------------
0x7fffff7ff000-0x7fffff8ff000 Stack
-----------------
```

The patch can indeed solve this problem, but the root cause is different from the UAF I submitted.

Comment 71 by adetaylor@google.com on Mon, Feb 8, 2021, 7:35 PM EST

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389, assuming that no problems showed up in dev.

Comment 72 by kolos@chromium.org on Tue, Feb 9, 2021, 3:36 AM EST

Cc: -kolos@chromium.org

Comment 73 by amyressler@google.com on Wed, Feb 10, 2021, 1:59 PM EST

Labels: -reward-topanel reward-unpaid reward-20000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 74 by thomasanderson@chromium.org on Wed, Feb 10, 2021, 2:21 PM EST

> The patch can indeed solve this problem, but the root cause is different from the UAF I submitted.

I agree. Since this issue is actually a stack overflow, it is different from UAF-class bugs.

Comment 75 by amyressler@google.com on Wed, Feb 10, 2021, 2:30 PM EST

Congratulations, Ryoya! The VRP Panel has decided to reward you $20,000 for this report. Thank you for your efforts and engagement on this issue.

Comment 76 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:37 PM EST

Labels: -Merge-Review-88 Merge-Approved-88

Approving merge to M88, branch 4324, assuming no problems showed up on dev. Please merge by the end of Thursday PST so that this gets picked up for next Tuesday's stable refresh.

Comment 77 by bugdroid on Wed, Feb 10, 2021, 5:42 PM EST

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cff3e4737dc1875b5cee27db95881e1d39167158

commit cff3e4737dc1875b5cee27db95881e1d39167158
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Wed Feb 10 22:41:13 2021

[Merge to M89] [XProto] Switch event queue from a std::list to a base::circular_deque

> This is needed as a prerequisite for [1]. It also improves performance
> a bit by replacing a node-based data structure with a flat one.
>
> [1] https://chromium-review.googlesource.com/c/chromium/src/+/2622521
>
> Change-Id: Ibe2e522f6c131876ed73793305524c25b42ab910
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2625784
> Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>

> Reviewed-by: Scott Violet <sky@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#844303}

TBR=sky

~~Bug: 1138143~~
Change-Id: I569ab57362c9ba7cff92691e4a3d55a7fc2869a2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2686765
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Auto-Submit: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#901}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/cff3e4737dc1875b5cee27db95881e1d39167158/ui/gfx/x/event.h
[modify] https://crrev.com/cff3e4737dc1875b5cee27db95881e1d39167158/ui/gfx/x/connection.cc
[modify] https://crrev.com/cff3e4737dc1875b5cee27db95881e1d39167158/ui/events/platform/x11/x11_event_source.cc
[modify] https://crrev.com/cff3e4737dc1875b5cee27db95881e1d39167158/ui/base/x/x11_util.cc
[modify] https://crrev.com/cff3e4737dc1875b5cee27db95881e1d39167158/ui/gfx/x/connection.h

Comment 78 by bugdroid on Wed, Feb 10, 2021, 5:45 PM EST
Labels: -merge-approved-88 merge-merged-4324 merge-merged-88

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/135a6e537f68c5000a61f970a96e1616b4af7f51

commit 135a6e537f68c5000a61f970a96e1616b4af7f51
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Wed Feb 10 22:45:10 2021

[Merge to M88] [XProto] Switch event queue from a std::list to a base::circular_deque

*** NOTE: THIS IS NOT A CLEAN MERGE ***

> This is needed as a prerequisite for [1]. It also improves performance
> a bit by replacing a node-based data structure with a flat one.
>
> [1] https://chromium-review.googlesource.com/c/chromium/src/+/2622521
>
> Change-Id: Ibe2e522f6c131876ed73793305524c25b42ab910
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2625784
> Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
> Reviewed-by: Scott Violet <sky@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#844303}

~~BUG=1138143~~
TBR=sky

Change-Id: I181af2c82d5552a3614747d8b4f6740583ec4ffe
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2687828
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Auto-Submit: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4324@{#2163}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/135a6e537f68c5000a61f970a96e1616b4af7f51/ui/gfx/x/event.h
[modify] https://crrev.com/135a6e537f68c5000a61f970a96e1616b4af7f51/ui/gfx/x/connection.cc
[modify] https://crrev.com/135a6e537f68c5000a61f970a96e1616b4af7f51/ui/events/platform/x11/x11_event_source.cc
[modify] https://crrev.com/135a6e537f68c5000a61f970a96e1616b4af7f51/ui/base/x/x11_util.cc
[modify] https://crrev.com/135a6e537f68c5000a61f970a96e1616b4af7f51/ui/gfx/x/connection.h

Comment 79 by bugdroid on Wed, Feb 10, 2021, 6:52 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/73721b793078b83953bb87945a11769c5f7ea394

commit 73721b793078b83953bb87945a11769c5f7ea394
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Wed Feb 10 23:52:01 2021

[Merge to M89] Avoid spinning a nested message loop for X11 clipboard

> BUG=443355,~~1138143~~,~~1161141~~,~~1161143~~,~~1161144~~,~~1161145~~,~~1161146~~,~~1161147~~,~~1161149~~,~~1161151~~,~~1161152~~
>
> Change-Id: I5c95a9d066683d18f344d694e517274e3ef7ccb4
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2622521
> Reviewed-by: Scott Violet <sky@chromium.org>
> Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#844318}

~~BUG=1138143~~
TBR=sky

Change-Id: I9260ecc7a3b06b97e54d03e6dbced0c4736f92c7
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2686346
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#905}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/73721b793078b83953bb87945a11769c5f7ea394/ui/base/x/selection_requestor_unittest.cc
[modify] https://crrev.com/73721b793078b83953bb87945a11769c5f7ea394/ui/base/x/selection_requestor.cc

Comment 80 by bugdroid on Wed, Feb 10, 2021, 6:55 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/202b40b9aee4971905c4bf7ec9be789ecc6b39ba

commit 202b40b9aee4971905c4bf7ec9be789ecc6b39ba
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Wed Feb 10 23:53:26 2021

[Merge to M88] Avoid spinning a nested message loop for X11 clipboard

*** NOTE: THIS IS NOT A CLEAN MERGE ***

> BUG=443355,~~1138143~~,~~1161141~~,~~1161143~~,~~1161144~~,~~1161145~~,~~1161146~~,~~1161147~~,~~1161149~~,~~1161151~~,~~1161152~~
>
> Change-Id: I5c95a9d066683d18f344d694e517274e3ef7ccb4
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2622521
> Reviewed-by: Scott Violet <sky@chromium.org>
> Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#844318}

~~BUG=1138143~~
TBR=sky

Change-Id: I7269ac8af7c91988a7d5520b3faf88dac89a577e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688137
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4324@{#2166}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/202b40b9aee4971905c4bf7ec9be789ecc6b39ba/ui/base/x/selection_requestor_unittest.cc
[modify] https://crrev.com/202b40b9aee4971905c4bf7ec9be789ecc6b39ba/ui/base/x/selection_requestor.cc

Comment 81 by work3...@gmail.com on Wed, Feb 10, 2021, 8:48 PM EST

Thank you for the reward!

Comment 82 by amyressler@google.com on Thu, Feb 11, 2021, 4:02 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 83 by adetaylor@google.com on Fri, Feb 12, 2021, 7:35 PM EST

Labels: Release-3-M88

Comment 84 by adetaylor@google.com on Fri, Feb 12, 2021, 7:38 PM EST

Cc: there...@gmail.com

~~Issue 1158135~~ has been merged into this issue.

Comment 85 by achuith@chromium.org on Thu, Feb 18, 2021, 8:59 PM EST

Labels: LTS-Security-NotApplicable-86

Comment 86 by amyressler@google.com on Mon, Feb 22, 2021, 4:31 PM EST

Labels: CVE-2021-21149 CVE_description-missing

Comment 87 by amyressler@google.com on Mon, Feb 22, 2021, 4:33 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 88 by collinbaker@chromium.org on Tue, Feb 23, 2021, 12:24 PM EST

Cc: -collinbaker@chromium.org

Comment 89 by sheriffbot on Sat, Apr 24, 2021, 1:50 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 90 by vsavu@google.com on Wed, Apr 28, 2021, 5:51 AM EDT

Labels: LTS-Security-86