Starred by 1 user

Owner:	thestig@chromium.org
CC:	adetaylor@chromium.org jschettler@chromium.org dcheng@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Printing
Modified:	Jan 14, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

reward-3000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-87
M-86
Target-86
merge-merged-4240
merge-merged-86
merge-merged-4280
merge-merged-87
Release-2-M86
CVE-2020-16003

Issue 1134960: Security: Use-after-free with using print dialog

Reported by chrom...@gmail.com on Sun, Oct 4, 2020, 12:22 AM EDT

Code

Chrome Version: 88.0.4281.0 canary
Operating System: All

REPRODUCTION CASE

1. Open the testcase
2. On print dialog, try to change from "Portrait" to "Landspace" option.
3. Reload the page

```
==1==ERROR: AddressSanitizer: heap-use-after-free on address 0x6150000bd400 at pc 0x55557c1c1f1a bp 0x7fffffffd300 sp 0x7fffffffd2f8
READ of size 8 at 0x6150000bd400 thread T0 (chrome)
==1==WARNING: invalid path to external symbolizer!
==1==WARNING: Failed to use and restart external symbolizer!
    #0 0x55557c1c1f19  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x26c6df19)
    #1 0x55556a55cdc5  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15008dc5)
    #2 0x55556a59523f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x1504123f)
    #3 0x55556a594abf  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15040abf)
    #4 0x55556a491f30  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14f3df30)
    #5 0x55556a596586  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15042586)
    #6 0x55556a509f2a  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14fb5f2a)
    #7 0x55557bf02c22  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x269aec22)
    #8 0x5555693b15af  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5d5af)
    #9 0x5555693b4a78  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e60a78)
    #10 0x55556954709d  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13ff309d)
    #11 0x5555693afa3f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5ba3f)
    #12 0x55555f220003  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x9ccc003)
    #13 0x7ffff63300b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

0x6150000bd400 is located 0 bytes inside of 512-byte region [0x6150000bd400,0x6150000bd600)
freed by thread T0 (chrome) here:
    #0 0x55555f21dd5d  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x9cc9d5d)
    #1 0x55556a55cdc5  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15008dc5)
    #2 0x55556a59523f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x1504123f)
    #3 0x55556a594abf  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15040abf)
    #4 0x55556a491f30  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14f3df30)
    #5 0x55556a596586  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15042586)
    #6 0x55556a509f2a  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14fb5f2a)
    #7 0x55557bf02c22  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x269aec22)
    #8 0x5555693b15af  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5d5af)
    #9 0x5555693b4a78  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e60a78)
    #10 0x55556954709d  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13ff309d)
    #11 0x5555693afa3f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5ba3f)
    #12 0x55555f220003  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x9ccc003)
    #13 0x7ffff63300b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

```
previously allocated by thread T0 (chrome) here:
    #0 0x55555f21d4fd  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x9cc94fd)
    #1 0x555579dff45a  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x248ab45a)
    #2 0x555579f99fad  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x24a45fad)
    #3 0x555579fc9253  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x24a75253)
    #4 0x555576aa0999  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x2154c999)
    #5 0x555576f28a86  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x219d4a86)
    #6 0x555576f1dac3  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x219c9ac3)
    #7 0x555576f2125f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x219cd25f)
    #8 0x555575442ddc  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x1feeeddc)
    #9 0x55557543ceed  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x1fee8eed)
    #10 0x55557727037b  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21d1c37b)
    #11 0x55557725dfac  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21d09fac)
    #12 0x555577261010  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21d0d010)
    #13 0x555577330028  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21ddc028)
    #14 0x555577231911  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21cdd911)
    #15 0x555577231020  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21cdd020)
    #16 0x55557722d03d  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x21cd903d)
    #17 0x555568462721  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x12f0e721)
    #18 0x55556a55cdc5  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15008dc5)
    #19 0x55556a59523f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x1504123f)
    #20 0x55556a594abf  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15040abf)
    #21 0x55556a491f30  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14f3df30)
    #22 0x55556a596586  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x15042586)
    #23 0x55556a509f2a  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x14fb5f2a)
    #24 0x55557bf02c22  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x269aec22)
    #25 0x5555693b15af  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5d5af)
    #26 0x5555693b4a78  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e60a78)
    #27 0x55556954709d  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13ff309d)
    #28 0x5555693afa3f  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x13e5ba3f)
    #29 0x55555f220003  (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x9ccc003)

SUMMARY: AddressSanitizer: heap-use-after-free (/home/lbstyle/Desktop/asan-linux-release-804487/chrome+0x26c6df19)
Shadow bytes around the buggy address:
  0x0c2a8000fa30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fa40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fa50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fa60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fa70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2a8000fa80:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fa90: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000faa0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fab0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8000fac0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8000fad0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==1==ABORTING
```

testcase.html
228 bytes View Download

screen.mov
2.4 MB View Download

Comment 1 by ClusterFuzz on Sun, Oct 4, 2020, 10:59 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5137842324176896.

Comment 2 by ClusterFuzz on Sun, Oct 4, 2020, 11:43 PM EDT

Testcase 5137842324176896 failed to reproduce the crash. Please inspect the program output at https://clusterfuzz.com/testcase?key=5137842324176896.

Comment 3 by dominickn@chromium.org on Sun, Oct 4, 2020, 11:50 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: thestig@chromium.org
Cc: dmazz...@chromium.org
Labels: Security_Severity-Medium OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: Internals>Printing

Hmm, looks like there might be some attempt to cache the |frame_| object when the change in orientation happens, so ClusterFuzz isn't sufficient to repro. Can you symbolize the crash?

+printing/accessibility folks.

Comment 4 by thestig@chromium.org on Tue, Oct 6, 2020, 2:18 AM EDT

Cc: -dmazz...@chromium.org

I can reproduce locally and symbolize it:

```
ERROR: AddressSanitizer: heap-use-after-free on address 0x61500000cd80 at pc 0x55dafd6625aa bp 0x7ffd93313440 sp 0x7ffd93313438
READ of size 8 at 0x61500000cd80 thread T0 (chrome)
    #0 0x55dafd6625a9 in base::DeleteHelper<printing::PrintRenderFrameHelper>::DoDelete(void const*) base/sequenced_task_runner_helpers.h:24:5
    #1 0x55dae6036630 in Run base/callback.h:100:12
    #2 0x55dae6036630 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:163:33
    #3 0x55dae60905bf in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:332:23
    #4 0x55dae608fce0 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:252:36
    #5 0x55dae5f180b3 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_default.cc:39:55
    #6 0x55dae6091d07 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:446:12
    #7 0x55dae5fc9018 in base::RunLoop::Run() base/run_loop.cc:124:14
    #8 0x55dafd2eb232 in content::RendererMain(content::MainFunctionParams const&) content/renderer/renderer_main.cc:256:16

0x61500000cd80 is located 0 bytes inside of 504-byte region [0x61500000cd80,0x61500000cf78)
freed by thread T0 (chrome) here:
    #0 0x55dad82de7ed in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x55dae6036630 in Run base/callback.h:100:12
    #2 0x55dae6036630 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:163:33
    #3 0x55dae60905bf in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:332:23
    #4 0x55dae608fce0 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:252:36
    #5 0x55dae5f180b3 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_default.cc:39:55
    #6 0x55dae6091d07 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:446:12
    #7 0x55dae5fc9018 in base::RunLoop::Run() base/run_loop.cc:124:14
    #8 0x55dafd2eb232 in content::RendererMain(content::MainFunctionParams const&) content/renderer/renderer_main.cc:256:16

previously allocated by thread T0 (chrome) here:
    #0 0x55dad82ddf8d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x55dafaadba8d in ChromeContentRendererClient::RenderFrameCreated(content::RenderFrame*) chrome/renderer/chrome_content_renderer_client.cc:516:3
    #2 0x55dafacc3a20 in content::RenderFrameImpl::Initialize(blink::WebFrame*) content/renderer/render_frame_impl.cc:2085:35
    #3 0x55dafacf552c in content::RenderFrameImpl::CreateChildFrame(blink::WebLocalFrame*, blink::mojom::TreeScopeType, blink::WebString const&, blink::WebString
const&, blink::FramePolicy const&, blink::WebFrameOwnerProperties const&, blink::mojom::FrameOwnerElementType) content/renderer/render_frame_impl.cc:4098:23
    #4 0x55daf6493aff in blink::WebLocalFrameImpl::CreateChildFrame(WTF::AtomicString const&, blink::HTMLFrameOwnerElement*)
third_party/blink/renderer/core/frame/web_local_frame_impl.cc:2008:16
    #5 0x55daf69a03c3 in blink::HTMLFrameOwnerElement::LoadOrRedirectSubframe(blink::KURL const&, WTF::AtomicString const&, bool)
third_party/blink/renderer/core/html/html_frame_owner_element.cc:574:43
    #6 0x55daf69969d9 in blink::HTMLFrameElementBase::OpenURL(bool) third_party/blink/renderer/core/html/html_frame_element_base.cc:106:3
    #7 0x55daf6998b24 in blink::HTMLFrameElementBase::SetNameAndOpenURL() third_party/blink/renderer/core/html/html_frame_element_base.cc:182:3
    #8 0x55daf50ec021 in blink::ContainerNode::NotifyNodeInserted(blink::Node&, blink::ContainerNode::ChildrenChangeSource)
third_party/blink/renderer/core/dom/container_node.cc:939:20
    ...
```

Comment 5 by thestig@chromium.org on Tue, Oct 6, 2020, 2:35 AM EDT

Cc: jschettler@chromium.org dcheng@chromium.org

Bisects to https://chromium.googlesource.com/chromium/src/+log/e1097b43..b0a990da, so it's likely r728794.

Comment 6 by meacer@google.com on Tue, Oct 6, 2020, 8:00 PM EDT

Labels: Security_Impact-Stable

Labeling based on comment #6.

Comment 7 by bugdroid on Wed, Oct 7, 2020, 1:47 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/6c2b1efa3d1ead8584489194a21183b954a3d184

commit 6c2b1efa3d1ead8584489194a21183b954a3d184
Author: Lei Zhang <thestig@chromium.org>
Date: Wed Oct 07 17:43:37 2020

Prevent double deletion in PrintRenderFrameHelper.

~~Bug: 1134960~~
Change-Id: I765cc3f1463fce4b8d7c2ca99f429031566a4645
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2454732
Reviewed-by: Jesse Schettler <jschettler@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Commit-Position: refs/heads/master@{#814756}

[modify] https://crrev.com/6c2b1efa3d1ead8584489194a21183b954a3d184/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/6c2b1efa3d1ead8584489194a21183b954a3d184/components/printing/renderer/print_render_frame_helper.h

Comment 8 by sheriffbot on Wed, Oct 7, 2020, 2:19 PM EDT

Labels: M-86 Target-86

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

Comment 9 Deleted

Comment 10 by chrom...@gmail.com on Wed, Oct 7, 2020, 4:51 PM EDT

I'm no longer able to reproduce this on the latest version of Chromium 88.0.4286.0 master@{#814796}. I will check it tomorrow on Canary.

Comment 11 by chrom...@gmail.com on Wed, Oct 7, 2020, 4:56 PM EDT

screen.mov
5.0 MB View Download

Comment 12 by thestig@chromium.org on Thu, Oct 8, 2020, 12:30 AM EDT

Status: Fixed (was: Assigned)

Thanks for the fix confirmation.

Comment 13 by sheriffbot on Thu, Oct 8, 2020, 3:07 PM EDT

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 14 by adetaylor@google.com on Sun, Oct 11, 2020, 9:07 PM EDT

Labels: reward-topanel

Comment 15 by sheriffbot on Mon, Oct 12, 2020, 3:33 PM EDT

Labels: Merge-Request-86

Requesting merge to beta M86 because latest trunk commit (814756) appears to be after beta branch point (800218).

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

Comment 16 by sheriffbot on Mon, Oct 12, 2020, 3:38 PM EDT

Labels: -Merge-Request-86 Hotlist-Merge-Review Merge-Review-86

This bug requires manual review: Request affecting a post-stable build
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), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 17 by thestig@chromium.org on Mon, Oct 12, 2020, 3:46 PM EDT

Cc: adetaylor@chromium.org

Comment 18 by thestig@chromium.org on Mon, Oct 12, 2020, 3:47 PM EDT

Labels: M-87

Needs a M87 merge as well.

Comment 19 by thestig@chromium.org on Tue, Oct 13, 2020, 1:50 PM EDT

Labels: Merge-Request-87

Comment 20 by adetaylor@google.com on Tue, Oct 13, 2020, 5:53 PM EDT

Labels: -Merge-Request-87 -Merge-Review-86 Merge-Approved-87 Merge-Approved-86

Approving merge to M87, branch 4280, and to M86, branch 4240.

(We don't always merge fixes back to the current stable branch but this looks very safe indeed.)

Comment 21 by thestig@chromium.org on Tue, Oct 13, 2020, 6:18 PM EDT

Merges in progress:

M86: https://chromium-review.googlesource.com/c/chromium/src/+/2469219
M87: https://chromium-review.googlesource.com/c/chromium/src/+/2468293

Comment 22 by bugdroid on Tue, Oct 13, 2020, 7:42 PM EDT

Labels: -merge-approved-87 merge-merged-87 merge-merged-4280

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/9b249e63a2aa7650aee7cefb0aaf85320a98c9c9

commit 9b249e63a2aa7650aee7cefb0aaf85320a98c9c9
Author: Lei Zhang <thestig@chromium.org>
Date: Tue Oct 13 23:41:09 2020

M87: Prevent double deletion in PrintRenderFrameHelper.

(cherry picked from commit 6c2b1efa3d1ead8584489194a21183b954a3d184)

Tbr: jschettler@chromium.org
~~Bug: 1134969~~
Change-Id: I765cc3f1463fce4b8d7c2ca99f429031566a4645
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2454732
Reviewed-by: Jesse Schettler <jschettler@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#814756}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2468293
Reviewed-by: Lei Zhang <thestig@chromium.org>
Cr-Commit-Position: refs/branch-heads/4280@{#351}
Cr-Branched-From: ea420fb963f9658c9969b6513c56b8f47efa1a2a-refs/heads/master@{#812852}

[modify] https://crrev.com/9b249e63a2aa7650aee7cefb0aaf85320a98c9c9/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/9b249e63a2aa7650aee7cefb0aaf85320a98c9c9/components/printing/renderer/print_render_frame_helper.h

Comment 23 by bugdroid on Tue, Oct 13, 2020, 8:01 PM EDT

Labels: -merge-approved-86 merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/7226741a00049dc88bee24dd7f935e6faa6e3197

commit 7226741a00049dc88bee24dd7f935e6faa6e3197
Author: Lei Zhang <thestig@chromium.org>
Date: Wed Oct 14 00:00:57 2020

M86: Prevent double deletion in PrintRenderFrameHelper.

(cherry picked from commit 6c2b1efa3d1ead8584489194a21183b954a3d184)

Tbr: jschettler@chromium.org
~~Bug: 1134969~~
Change-Id: I765cc3f1463fce4b8d7c2ca99f429031566a4645
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2454732
Reviewed-by: Jesse Schettler <jschettler@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#814756}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2469219
Reviewed-by: Lei Zhang <thestig@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1235}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/7226741a00049dc88bee24dd7f935e6faa6e3197/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/7226741a00049dc88bee24dd7f935e6faa6e3197/components/printing/renderer/print_render_frame_helper.h

Comment 24 by thestig@chromium.org on Tue, Oct 13, 2020, 8:02 PM EDT

Labels: -Hotlist-Merge-Review

Comment 25 by adetaylor@google.com on Wed, Oct 14, 2020, 6:13 PM EDT

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 26 by adetaylor@google.com on Wed, Oct 14, 2020, 6:23 PM EDT

Congratulations, the VRP panel has decided to award $3000 for this bug.

Comment 27 by adetaylor@google.com on Fri, Oct 16, 2020, 11:20 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 28 by adetaylor@google.com on Mon, Oct 19, 2020, 11:09 PM EDT

Labels: Release-2-M86

Comment 29 by adetaylor@google.com on Sun, Dec 6, 2020, 12:59 AM EST

Labels: CVE-2020-16003 CVE_description-missing

Comment 30 by jschettler@chromium.org on Mon, Dec 7, 2020, 11:00 AM EST

There's a chance this has resurfaced as ~~issue 1151726~~.

Comment 31 by adetaylor@google.com on Thu, Jan 7, 2021, 2:03 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Thu, Jan 14, 2021, 1:51 PM EST

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