☆ Starred by 3 users

Owner:	afakhry@chromium.org
CC:	kyleshima@chromium.org dgagnon@chromium.org gzadina@chromium.org conniekxu@chromium.org dhadd...@chromium.org ceb@chromium.org amyressler@chromium.org minch@chromium.org michelefan@chromium.org
Status:	Fixed *(Closed)*
Components:	----
Modified:	Oct 8, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome, Lacros
Pri:	1
Type:	Bug-Security

reward-10000
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-97
Restrict-AddIssueComment-scr2b-migration
external_security_report
FoundIn-97
Security_Impact-Extended
merge-merged-4692
merge-merged-97
sw-b-migration-candidate
LTS-NotApplicable-96
Release-0-M97
CVE-2022-0098
migrated-to-b-252341075

Issue 1273609: heap-use-after-free video_recording_watcher.cc:673:7

Reported by rheza...@gmail.com on Wed, Nov 24, 2021, 4:14 PM EST

Code

Only users with scr2b-migration permission or issue reporter may comment.

This issue has moved to b/252341075. Updates should be posted in b/252341075.

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36

Steps to reproduce the problem:
I will post the PoC and video soon

What is the expected behavior?
not crash

What went wrong?

```
=================================================================
==27029==ERROR: AddressSanitizer: heap-use-after-free on address 0x61500015a070 at pc 0x55e064438e85 bp
0x7fff14401390 sp 0x7fff14401388
READ of size 4 at 0x61500015a070 thread T0 (chrome)
==27029==WARNING: invalid path to external symbolizer!
==27029==WARNING: Failed to use and restart external symbolizer!
    #0 0x55e064438e84 in width ./../../ui/gfx/geometry/size.h:49:40
    #1 0x55e064438e84 in SizeF ./../../ui/gfx/geometry/size_f.h:30:39
    #2 0x55e064438e84 in ash::VideoRecordingWatcher::UpdateCursorOverlayNow(gfx::PointF const&)
./../../ash/capture_mode/video_recording_watcher.cc:673:7
    #3 0x55e05a6529f3 in Run ./../../base/callback.h:142:12
    #4 0x55e05a6529f3 in base::OneShotTimer::RunUserTask() ./../../base/timer/timer.cc:290:19
    #5 0x55e05a5fbae1 in Run ./../../base/callback.h:142:12
    #6 0x55e05a5fbae1 in base::DefaultDelayedTaskHandleDelegate::RunTask(base::OnceCallback<void ()>)
./../../base/task/default_delayed_task_handle_delegate.cc:36:24
    #7 0x55e05a5fbdc2 in Invoke<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >
./../../base/bind_internal.h:533:12
    #8 0x55e05a5fbdc2 in MakeItSo<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> > ./../../base/bind_internal.h:728:5
    #9 0x55e05a5fbdc2 in RunImpl<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
std::__1::tuple<base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, 0UL, 1UL>
./../../base/bind_internal.h:781:12
    #10 0x55e05a5fbdc2 in base::internal::Invoker<base::internal::BindState<void
(base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, void
()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:750:12
    #11 0x55e05a5b66d6 in Run ./../../base/callback.h:142:12
    #12 0x55e05a5b66d6 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32

    #13 0x55e05a5efd03 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:358:29)>
./../../base/task/common/task_annotator.h:73:5
```

```
./../../base/task/common/task_annotator.h:73:5
    #14 0x55e05a5efd03 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356:21
    #15 0x55e05a5ef552 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #16 0x55e05a5f08c1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #17 0x55e05a72edfd in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_libevent.cc:195:55
    #18 0x55e05a5f0f7e in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #19 0x55e05a52f3ec in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:140:14
    #20 0x55e0511f6727 in content::BrowserMainLoop::RunMainMessageLoop()
./../../content/browser/browser_main_loop.cc:1001:18
    #21 0x55e0511fac05 in content::BrowserMainRunnerImpl::Run()
./../../content/browser/browser_main_runner_impl.cc:153:15
    #22 0x55e0511f0d67 in content::BrowserMain(content::MainFunctionParams)
./../../content/browser/browser_main.cc:30:28
    #23 0x55e05a310859 in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:646:10
    #24 0x55e05a313356 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./../../content/app/content_main_runner_impl.cc:1159:10
    #25 0x55e05a312732 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1026:12
    #26 0x55e05a30cf9b in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:398:36
    #27 0x55e05a30d601 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:426:10
    #28 0x55e04d0f95da in ChromeMain ./../../chrome/app/chrome_main.cc:172:12
    #29 0x7f52516080b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

0x61500015a070 is located 240 bytes inside of 504-byte region [0x615000159f80,0x61500015a178)
freed by thread T0 (chrome) here:
    #0 0x55e04d0f761d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/asan/asan_new_delete.cpp:152:3
    #1 0x55e05a5b66d6 in Run ./../../base/callback.h:142:12
    #2 0x55e05a5b66d6 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
    #3 0x55e05a5efd03 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:358:29)>
./../../base/task/common/task_annotator.h:73:5
    #4 0x55e05a5efd03 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356:21
    #5 0x55e05a5ef552 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #6 0x55e05a5f08c1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #7 0x55e05a72edfd in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_libevent.cc:195:55

    #8 0x55e05a5f0f7e in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #9 0x55e05a52f3ec in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:140:14
    #9 0x55e05a52f3ec in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:140:14
    #10 0x55e0511f6727 in content::BrowserMainLoop::RunMainMessageLoop()
./../../content/browser/browser_main_loop.cc:1001:18
    #11 0x55e0511fac05 in content::BrowserMainRunnerImpl::Run()
./../../content/browser/browser_main_runner_impl.cc:153:15
    #12 0x55e0511f0d67 in content::BrowserMain(content::MainFunctionParams)
./../../content/browser/browser_main.cc:30:28
    #13 0x55e05a310859 in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:646:10
    #14 0x55e05a313356 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./../../content/app/content_main_runner_impl.cc:1159:10
    #15 0x55e05a312732 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1026:12
    #16 0x55e05a30cf9b in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:398:36
    #17 0x55e05a30d601 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:426:10
    #18 0x55e04d0f95da in ChromeMain ./../../chrome/app/chrome_main.cc:172:12
    #19 0x7f52516080b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 (chrome) here:
    #0 0x55e04d0f6dbd in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/asan/asan_new_delete.cpp:95:3
    #1 0x55e06200a40c in views::NativeWidgetAura::NativeWidgetAura(views::internal::NativeWidgetDelegate*)
./../../ui/views/widget/native_widget_aura.cc:106:15
    #2 0x55e066d74782 in BrowserFrameAsh::BrowserFrameAsh(BrowserFrame*, BrowserView*)
./../../chrome/browser/ui/views/frame/browser_frame_ash.cc:76:7
    #3 0x55e066d74662 in NativeBrowserFrameFactory::Create(BrowserFrame*, BrowserView*)
./../../chrome/browser/ui/views/frame/native_browser_frame_factory_chromeos.cc:12:14
    #4 0x55e066c8b290 in BrowserFrame::InitBrowserFrame() ./../../chrome/browser/ui/views/frame/browser_frame.cc:91:7
    #5 0x55e066d6f2f1 in BrowserWindow::CreateBrowserWindow(std::__1::unique_ptr<Browser,
std::__1::default_delete<Browser> >, bool, bool) ./../../chrome/browser/ui/views/frame/browser_window_factory.cc:54:18
    #6 0x55e0660f9e6d in CreateBrowserWindow ./../../chrome/browser/ui/browser.cc:307:10
    #7 0x55e0660f9e6d in Browser::Browser(Browser::CreateParams const&) ./../../chrome/browser/ui/browser.cc:524:29
    #8 0x55e0660f8b6c in Browser::Create(Browser::CreateParams const&) ./../../chrome/browser/ui/browser.cc:444:14
    #9 0x55e06611539e in chrome::OpenEmptyWindow(Profile*, bool) ./../../chrome/browser/ui/browser_commands.cc:504:22
    #10 0x55e06611513b in chrome::NewEmptyWindow(Profile*, bool) ./../../chrome/browser/ui/browser_commands.cc:0:0
    #11 0x55e06679e384 in BrowserShortcutShelfItemController::ItemSelected(std::__1::unique_ptr<ui::Event,
std::__1::default_delete<ui::Event> >, long, ash::ShelfLaunchSource, base::OnceCallback<void (ash::ShelfAction,
std::__1::vector<ash::ShelfItemDelegate::AppMenuItem, std::__1::allocator<ash::ShelfItemDelegate::AppMenuItem> >)>,
base::RepeatingCallback<bool (aura::Window*)> const&)
./../../chrome/browser/ui/ash/shelf/browser_shortcut_shelf_item_controller.cc:126:44
    #12 0x55e06472f089 in ash::ShelfView::ButtonPressed(views::Button*, ui::Event const&, views::InkDrop*)
./../../ash/shelf/shelf_view.cc:801:42
    #13 0x55e061e4ab7a in views::Button::DefaultButtonControllerDelegate::NotifyClick(ui::Event const&)
./../../ui/views/controls/button/button.cc:66:13
    #14 0x55e061e527d6 in views::ButtonController::OnMouseReleased(ui::MouseEvent const&)
./../../ui/views/controls/button/button_controller.cc:0:34
    #15 0x55e0646deb06 in ash::ShelfAppButton::OnMouseReleased(ui::MouseEvent const&)
./../../ash/shelf/shelf_app_button.cc:619:16
    #16 0x55e061e1fbbf in ui::ScopedTargetHandler::OnEvent(ui::Event*) ./../../ui/events/scoped_target_handler.cc:28:24
    #17 0x55e05d5feca5 in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
./../../ui/events/event_dispatcher.cc:190:12

    #18 0x55e05d5fe264 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:139:5
    #19 0x55e05d5fdd3c in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
```

```
   #19 0x55e05d5fdd2c in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:83:14
   #20 0x55e05d5fda99 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:55:15
   #21 0x55e061fb118a in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&)
./../../ui/views/widget/root_view.cc:484:9
   #22 0x55e061fc82ce in views::Widget::OnMouseEvent(ui::MouseEvent*) ./../../ui/views/widget/widget.cc:1544:20
   #23 0x55e05d5feca5 in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
./../../ui/events/event_dispatcher.cc:190:12
   #24 0x55e05d5fe264 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:139:5
   #25 0x55e05d5fdd2c in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:83:14
   #26 0x55e05d5fda99 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
./../../ui/events/event_dispatcher.cc:55:15
   #27 0x55e0606d66ae in ui::EventProcessor::OnEventFromSource(ui::Event*) ./../../ui/events/event_processor.cc:49:17
   #28 0x55e05d601eac in ui::EventSource::DeliverEventToSink(ui::Event*) ./../../ui/events/event_source.cc:117:16
   #29 0x55e05d602365 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./../../ui/events/event_source.cc:65:14
   #30 0x55e05394b6ce in ui::EventRewriterChromeOS::RewriteMouseButtonEvent(ui::MouseEvent const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./../../ui/chromeos/events/event_rewriter_chromeos.cc:1274:12

SUMMARY: AddressSanitizer: heap-use-after-free (/home/dadang/asan/chromeOS/asan-linux-release-
945044/chrome+0x24bb1e84)
Shadow bytes around the buggy address:
  0x0c2a800233b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a800233c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a800233d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a800233e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a800233f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c2a80023400: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd
  0x0c2a80023410: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a80023420: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c2a80023430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a80023440: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a80023450: 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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==27029==ABORTING
```

Did this work before? N/A

Chrome version: 96.0.4664.45 Channel: stable
OS Version:

Tested on asan-linux-release-945044.zip - Version 98.0.4728.0 (Developer Build) (64-bit)

Comment 1 by sheriffbot on Wed, Nov 24, 2021, 4:15 PM EST

Labels: external_security_report

Comment 2 by rheza...@gmail.com on Wed, Nov 24, 2021, 4:53 PM EST

Step to reproduce:

(1) Launch ChromeOS in Ubuntu
(2) F5 -> create new Desk -> fill name
(3) Open chrome and Open screen capture -> screen record -> take window screenshot
(4) Close chrome

[Deleted] **1273609.mp4**

Comment 3 by rheza...@gmail.com on Wed, Nov 24, 2021, 5:06 PM EST

The video is over 10MB, so I uploaded to Google Drive:
https://drive.google.com/file/d/1jr92sbGiOMCaA0w1bayTcETDTBGnL4Wq/view?usp=sharing

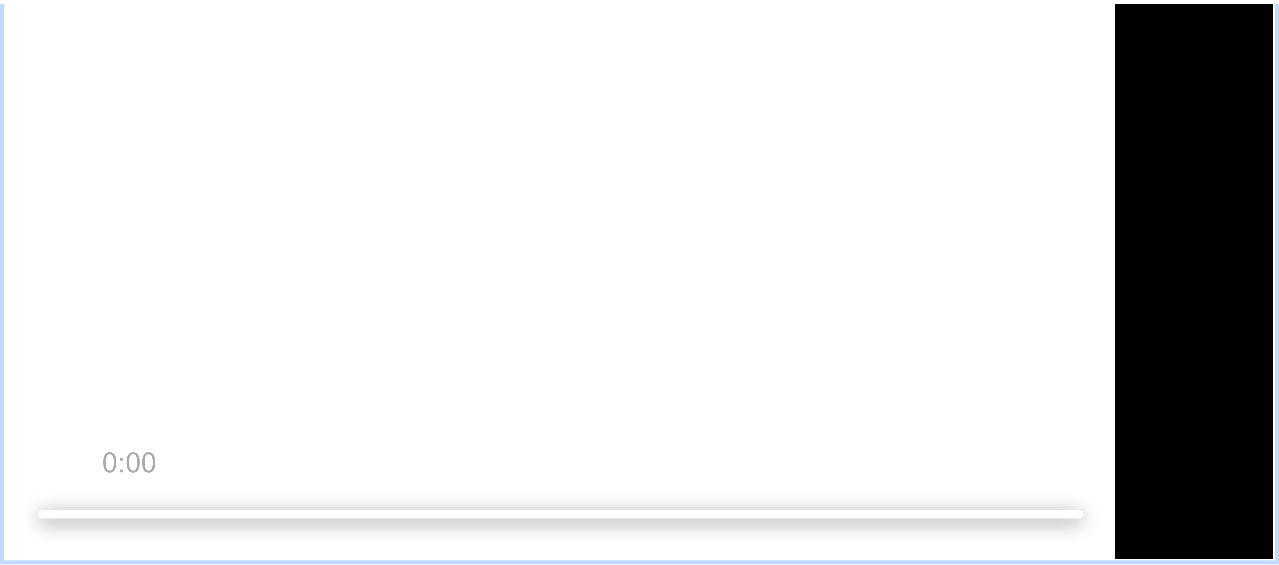
Comment 4 by rheza...@gmail.com on Wed, Nov 24, 2021, 6:22 PM EST

Another step to reproduce:

(1) Launch ChromeOS in Ubuntu
(2) Open chrome and Open screen capture -> screen record -> take window screenshot
(3) Open Print dialog (ctrl+p) then cancel print
(4) Close chrome

1273609_b_6.20.8.mp4
6.9 MB View Download

[redacted]

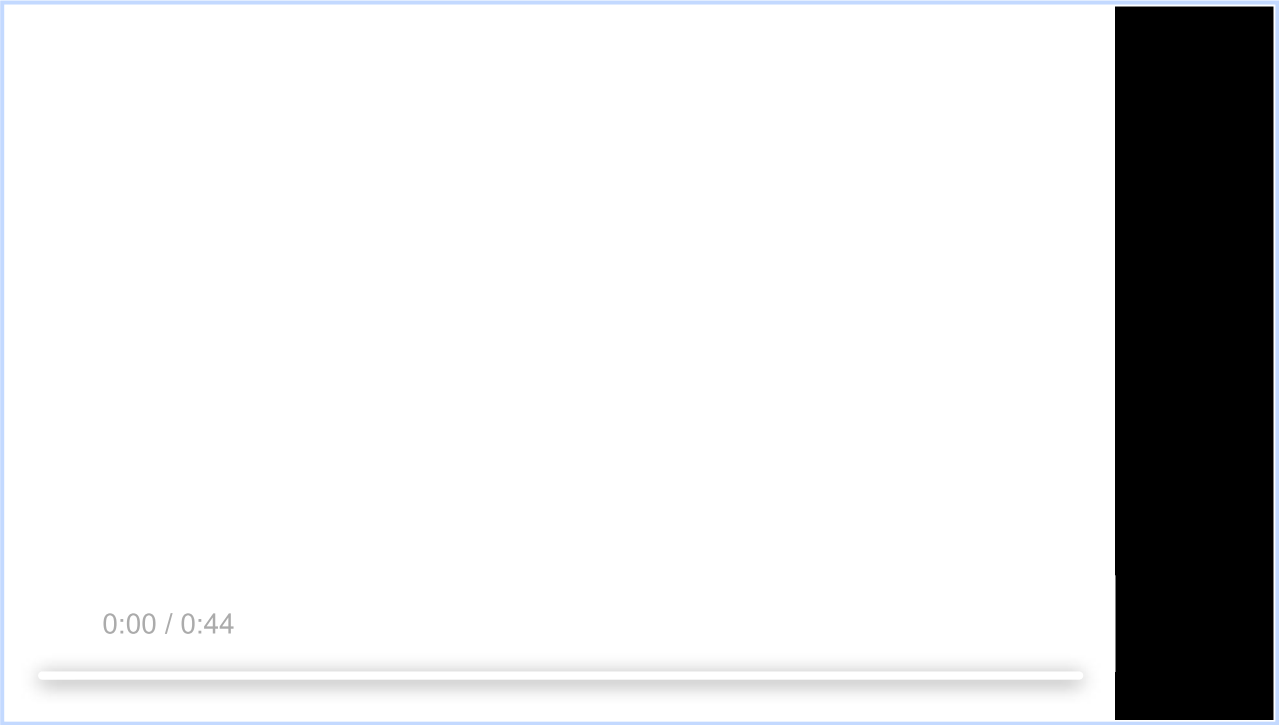


Comment 5 by rheza...@gmail.com on Thu, Nov 25, 2021, 3:16 PM EST

Another simplest to reproduce:

(1) Open chrome and open new tab 1 and 2
(2) Open screen capture -> screen record -> take window screenshot
(3) close tab 1 then tab 2

1273609_c.webm
3.8 MB View Download



Comment 6 by rsesek@chromium.org on Mon, Nov 29, 2021, 3:57 PM EST

Status: Assigned (was: Unconfirmed)
Owner: afakhry@chromium.org

Labels: -OS-Linux Security_Severity-High FoundIn-96 OS-Chrome OS-Lacros Pri-1
Components: UI>Shell>ScreenCapture

Comment 7 by sheriffbot on Mon, Nov 29, 2021, 4:01 PM EST

Labels: Security_Impact-Extended

Comment 8 by afakhry@chromium.org on Mon, Nov 29, 2021, 9:53 PM EST

Status: Started (was: Assigned)
Cc: gzadina@chromium.org conniekxu@chromium.org minch@chromium.org michelefan@chromium.org

I can repro using the steps in comment#4 but not comment#5. Also note the step to open the print dialog is not needed.

Comment 9 by Git Watcher on Tue, Nov 30, 2021, 12:37 PM EST

Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/fccc5919f3edb3b7e6edad4641d6479628976714

commit fccc5919f3edb3b7e6edad4641d6479628976714
Author: Ahmed Fakhry <afakhry@chromium.org>
Date: Tue Nov 30 17:36:38 2021

capture_mode: Fix UAF when recorded window is closed

Shutting down the VideoRecordingWatcher should properly
reset all scoped elements, and stop observing everything.
This is because the shutdown may be due to the destruction
of the window being recorded, so we can no longer access it.
But the VideoRecordingWatcher object is kept alive until
recording is actually finalized.

~~Fixed: 1273609~~
Test: Manually, modified a test such that it fails ASAN
without the fix.

Change-Id: If9869bfb2f27f6813546661c8bc27dbe9540f3c6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3308095
Commit-Queue: Ahmed Fakhry <afakhry@chromium.org>
Reviewed-by: Min Chen <minch@chromium.org>
Cr-Commit-Position: refs/heads/main@{#946519}

[modify] https://crrev.com/fccc5919f3edb3b7e6edad4641d6479628976714/ash/capture_mode/video_recording_watcher.cc
[modify] https://crrev.com/fccc5919f3edb3b7e6edad4641d6479628976714/ash/capture_mode/capture_mode_unittests.cc
[modify] https://crrev.com/fccc5919f3edb3b7e6edad4641d6479628976714/ash/capture_mode/video_recording_watcher.h

Comment 10 by sheriffbot on Tue, Nov 30, 2021, 12:41 PM EST

Labels: reward-topanel

Comment 11 by sheriffbot on Tue, Nov 30, 2021, 12:47 PM EST

Labels: Target-96 M-96

Setting milestone and target because of high severity.

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

Comment 12 by afakhry@chromium.org on Tue, Nov 30, 2021, 12:47 PM EST

Labels: Merge-Request-97

Comment 13 by sheriffbot on Tue, Nov 30, 2021, 1:41 PM EST

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

Comment 14 Deleted

Comment 15 by rheza...@gmail.com on Tue, Nov 30, 2021, 2:49 PM EST

Sorry I deleted #c14.

Thank you for expedited fixing this issue. I've tested on 946525 ~10 times with step #c5 and have no longer crashed.

Comment 16 by amyressler@chromium.org on Tue, Nov 30, 2021, 3:11 PM EST

hi afakhry@, you don't have to manually request a merge review as the bot will do that soon since you marked it fixed when you landed your CL :)

That being said, I'd like to give this a bit more time on canary before approving merge, so it will miss today's m97/beta cut.

I'll re-assess for merge review tomorrow or Thursday and we should be able to hopefully get this fix in next week's stable respin (which is being cut EOD Friday).

Please let me know if you have any issues or concerns with this.

Comment 17 by afakhry@chromium.org on Tue, Nov 30, 2021, 5:44 PM EST

Cc: amyressler@chromium.org

Re#16: Thank you so much, and take your time.

Comment 18 by ceb@google.com on Wed, Dec 1, 2021, 11:32 AM EST

Labels: -Merge-Request-97 Merge-Review-96

Manually updating with Merge Questionnaire.

Merge review required: M97 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:

1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative? https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.

Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

Comment 19 by ceb@google.com on Wed, Dec 1, 2021, 11:33 AM EST

Labels: Merge-Review-97 M-97

Also adding M-97 label, since this will need to be merged to both branches.

Comment 20 by afakhry@chromium.org on Wed, Dec 1, 2021, 11:55 AM EST

Cc: dhadd...@chromium.org ceb@chromium.org dgagnon@chromium.org

1. This fixes a use-after-free security issue.
2. https://chromium-review.googlesource.com/c/chromium/src/+/3308095,
3. Yes, initially landed in 98.0.4740.0,
4. Not a new feature,
5. +dhaddock@
6. No manual verification should be needed.

Comment 21 by dhadd...@chromium.org on Wed, Dec 1, 2021, 4:52 PM EST

LGTM

Comment 22 by dgagnon@google.com on Wed, Dec 1, 2021, 8:57 PM EST

Labels: -Merge-Review-96 Merge-Approved-96

Merge approved for M96

Comment 23 by ceb@google.com on Thu, Dec 2, 2021, 11:33 AM EST

Labels: -Merge-Review-97 Merge-Approved-97

Merge approved for M97.

Comment 24 by afakhry@chromium.org on Thu, Dec 2, 2021, 12:20 PM EST

rhezashan@ Are you sure this issue repros on M-96? I tried multiple times, and it doesn't seem to fail at all.

Comment 25 by Git Watcher on Thu, Dec 2, 2021, 12:39 PM EST

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cefa9f2fcb175fd6a21bd616bd5ce73bb90a9ee1

commit cefa9f2fcb175fd6a21bd616bd5ce73bb90a9ee1
Author: Ahmed Fakhry <afakhry@chromium.org>
Date: Thu Dec 02 17:38:20 2021

[Merge to M-97] capture_mode: Fix UAF when recorded window is closed

Shutting down the VideoRecordingWatcher should properly
reset all scoped elements, and stop observing everything.
This is because the shutdown may be due to the destruction
of the window being recorded, so we can no longer access it.
But the VideoRecordingWatcher object is kept alive until
recording is actually finalized.

~~Fixed: 1273609~~
Test: Manually, modified a test such that it fails ASAN

Test: Manually, modified a test such that it fails ASAN
without the fix.

(cherry picked from commit fccc5919f3edb3b7e6edad4641d6479628976714)

Change-Id: If9869bfb2f27f6813546661c8bc27dbe9540f3c6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3308095
Commit-Queue: Ahmed Fakhry <afakhry@chromium.org>
Reviewed-by: Min Chen <minch@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#946519}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3312909
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Auto-Submit: Ahmed Fakhry <afakhry@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4692@{#650}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify] https://crrev.com/cefa9f2fcb175fd6a21bd616bd5ce73bb90a9ee1/ash/capture_mode/video_recording_watcher.cc
[modify] https://crrev.com/cefa9f2fcb175fd6a21bd616bd5ce73bb90a9ee1/ash/capture_mode/capture_mode_unittests.cc
[modify] https://crrev.com/cefa9f2fcb175fd6a21bd616bd5ce73bb90a9ee1/ash/capture_mode/video_recording_watcher.h

Comment 26 by rheza...@gmail.com on Thu, Dec 2, 2021, 1:03 PM EST

Afakhary@,

I apologize #c14 deleted because I tested with wrong step and version. Your fix was good and it doesn't crash anymore. Sorry for confused.

Comment 27 by afakhry@chromium.org on Thu, Dec 2, 2021, 1:24 PM EST

Sorry, I mean your bug description (i.e. comment #0) says: Chrome/96.0.4664.45. I don't think this UAF exists in M-96. I'm asking to see if I need to actually merge to M-96.

Comment 28 by rheza...@gmail.com on Thu, Dec 2, 2021, 1:31 PM EST

Oh.. i see. Chrome/96.0.4664.45 (my Ubuntu Chrome browser version) it comes automatically from template when I submit/open new report from external_security_report. I apologize didn't set up correctly.

Comment 29 by afakhry@chromium.org on Thu, Dec 2, 2021, 1:34 PM EST

Labels: -M-96 -Merge-Approved-96 -Target-96 -FoundIn-96 FoundIn-97

Ok, great. No need to merge to M-96 then. Thanks for clarifying.

Comment 30 by amyressler@google.com on Mon, Dec 6, 2021, 6:16 PM EST

Labels: -reward-topanel reward-unpaid reward-10000

*** 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.

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

Comment 31 by amyressler@chromium.org on Mon, Dec 6, 2021, 6:40 PM EST

Congratulations on another one! The VRP Panel has decided to award you $10,000 for this report. Thank you for your efforts and excellent work!

Comment 32 by dhadd...@chromium.org on Mon, Dec 6, 2021, 8:16 PM EST

Cc: kyleshima@chromium.org

Comment 33 by rheza...@gmail.com on Mon, Dec 6, 2021, 9:53 PM EST

Thanks everyone. Happy winter holidays

Comment 34 by amyressler@google.com on Tue, Dec 7, 2021, 2:17 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 35 by amyressler@chromium.org on Tue, Jan 4, 2022, 11:58 AM EST

Labels: Release-0-M97

Comment 36 by amyressler@google.com on Tue, Jan 4, 2022, 1:33 PM EST

Labels: CVE-2022-0098 CVE_description-missing

Comment 37 by gmpritchard@google.com on Thu, Jan 6, 2022, 10:31 AM EST

Labels: LTS-NotApplicable-96

Comment 38 by sheriffbot on Tue, Mar 8, 2022, 1:30 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

Comment 39 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 40 by chromeos-software-bugbot on Tue, Oct 4, 2022, 10:32 PM EDT

Labels: sw-b-migration-candidate

Comment 41 by chromeos-software-bugbot on Sat, Oct 8, 2022, 9:30 PM EDT

Labels: Restrict-AddIssueComment-SCr2B-migration migrated-to-b-252341075
Components: -UI>Shell>ScreenCapture

Migrated to https://issuetracker.google.com/issues/252341075