☆ Starred by 5 users

Owner:	fangzhoug@chromium.org
CC:	----
Status:	Fixed *(Closed)*
Components:	Internals>Ozone
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
reward-7000
FoundIn-99
Release-0-M101
CVE-2022-1487

Issue 1304368: Security: UAF in ui/ozone/platform/wayland/host/wayland_window.cc

Reported by rzin...@gmail.com on Tue, Mar 8, 2022, 3:20 PM EST

Code

VULNERABILITY DETAILS

Use-after-free in ui/ozone/platform/wayland/host/wayland_window.cc

VERSION

Chrome Version: 101.0.4903.0
Operating System: Ubuntu 20.04 LTS

REPRODUCTION CASE

Run the test XdgVersionStableTest/WaylandWindowTest.DispatchesLocatedEventsToCapturedWindow/0 under asan.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser

CREDIT INFORMATION

Reporter credit: Sri

xdg_waylandwindow.log
8.2 KB View Download

Comment 1 by sheriffbot on Tue, Mar 8, 2022, 3:21 PM EST

Labels: external_security_report

Comment 2 by dcheng@chromium.org on Wed, Mar 9, 2022, 1:39 PM EST

~~Issue 1304370~~ has been merged into this issue.

Comment 3 by bookholt@chromium.org on Wed, Mar 9, 2022, 6:32 PM EST

Status: Assigned (was: Unconfirmed)
Owner: fangzhoug@chromium.org
Labels: FoundIn-99 OS-Linux Pri-2
Components: Internals>Ozone

I'm able to reproduce this crash at tip of tree from a Linux ASAN build.

This appears to be a UAF in browser process affecting Linux with Wayland. From a quick read of the ASAN report, some cleanup is initiated at [1] and then destructors are called immediately again to free objects going out of scope at the end of the function.

I don't know this subsystem, but I think this warrants an audit of calls to CreateWaylandWindowWithParams [2] to trace

I don't know this subsystem, but I think this warrants an audit of calls to CreateWaylandWindowWithParams [2] to trace how these objects are freed.

It's not immediately clear what an exploit looks like for this bug; the audit mentioned above is likely the only way to assess exploitability. @rzintct you are most welcome and encouraged to do such an audit and append those findings here, which would be incorporated into VRP reward decisions. @fangzhoug can you also PTAL to assess severity per [3]?

[1]
https://source.chromium.org/chromium/chromium/src/+/main:ui/ozone/platform/wayland/host/wayland_window_unittest.cc;l=1524;drc=289400c4507ba73b9ab67b2ed09ce639b955fea2
[2]
https://source.chromium.org/chromium/chromium/src/+/main:ui/ozone/platform/wayland/host/wayland_window_unittest.cc;l=192;drc=359c4471ef9ffdf94d1080815d51f28ce0302b94;bpv=1;bpt=1
[3] https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/severity-guidelines.md

Comment 4 by sheriffbot on Wed, Mar 9, 2022, 6:32 PM EST

Labels: Security_Impact-Stable

Comment 5 by fangzhoug@chromium.org on Thu, Mar 10, 2022, 2:00 PM EST

Labels: Security_Severity-Low

```
==3119674==ERROR: AddressSanitizer: heap-use-after-free on address 0x6140000012c0 at pc 0x562400f13a94 bp 0x7ffcd8c684d0 sp 0x7ffcd8c684c8
READ of size 8 at 0x6140000012c0 thread T0
    #0 0x562400f13a93 in ui::WaylandWindow::child_window() const ui/ozone/platform/wayland/host/wayland_window.h:115:48
    #1 0x562400f66400 in ui::WaylandWindow::~WaylandWindow() ui/ozone/platform/wayland/host/wayland_window.cc:94:41
    #2 0x562400f0e32a in ui::WaylandPopup::~WaylandPopup() ui/ozone/platform/wayland/host/wayland_popup.cc:35:29
    #3 0x562400f0e378 in ui::WaylandPopup::~WaylandPopup() ui/ozone/platform/wayland/host/wayland_popup.cc:35:29
    #4 0x5623fc02e5f2 in std::__1::default_delete<ui::WaylandWindow>::operator()(ui::WaylandWindow*) const buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
    #5 0x5623fc02e47f in std::__1::unique_ptr<ui::WaylandWindow, std::__1::default_delete<ui::WaylandWindow> >::reset(ui::WaylandWindow*) buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:315:7
    #6 0x5623fc014d18 in std::__1::unique_ptr<ui::WaylandWindow, std::__1::default_delete<ui::WaylandWindow> >::~unique_ptr() buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:269:19
    #7 0x5623fc244bcf in ui::WaylandWindowTest_DispatchesLocatedEventsToCapturedWindow_Test::TestBody() ui/ozone/platform/wayland/host/wayland_window_unittest.cc:1525:1
    #8 0x5623fd77f44f in void testing::internal::HandleSehExceptionsInMethodIfSupported<testing::Test, void>(testing::Test*, void (testing::Test::*)(), char const*) third_party/googletest/src/googletest/src/gtest.cc:2656:10
...
```

I think this if clause[1] should be moved to ~WaylandPopup() as popup is the only WaylandWindow variant that can make use of this. Doing so does resolve the crash.
But I'm not sure why it is a UAF to access parent_window()'s member in this dtor, the parent_window() (which is the window_ in that unittest) is still alive when this happens.

[1]https://source.chromium.org/chromium/chromium/src/+/main:ui/ozone/platform/wayland/host/wayland_window.cc;l=94;drc=359c4471ef9ffdf94d1080815d51f28ce0302b94;bpv=0;bpt=1

I'm not sure about the severity though. This code is running on LaCrOS and custom built for linux w/ Wayland so I'd think it's low.

Comment 6 by fangzhoug@chromium.org on Thu, Mar 10, 2022, 8:10 PM EST

Sorry I mistook. Moving to ~WaylandPopup() doesn't resolve it.

Comment 7 by fangzhoug@chromium.org on Thu, Mar 10, 2022, 8:30 PM EST

Ah I see what's wrong. Silly. Patch on https://chromium-review.googlesource.com/c/chromium/src/+/3517354, to trigger this bug, the parent window needs to be closed before its child window, e.g. toplevel window closes before popup, root popup closes before nested popup.

Comment 8 by Git Watcher on Sun, Mar 13, 2022, 8:08 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e161e3691f6807e64a8f51e454d3ac2fd2f292d2

commit e161e3691f6807e64a8f51e454d3ac2fd2f292d2
Author: Kramer Ge <fangzhoug@chromium.org>
Date: Mon Mar 14 00:07:44 2022

[Ozone/Wayland]WaylandWindow's parent_window use-after-free

To insure the child_window access after parent's destruct doesn't have
UAF, clear the parent_window of the child in dtor.

Change-Id: I18ea65a76e715e98747588fbe75e1a37cbbe199c
~~Bug: 1304368~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3517354
Reviewed-by: Maksim Sisov <msisov@igalia.com>
Commit-Queue: Kramer Ge <fangzhoug@chromium.org>
Cr-Commit-Position: refs/heads/main@{#980391}

[modify]
https://crrev.com/e161e3691f6807e64a8f51e454d3ac2fd2f292d2/ui/ozone/platform/wayland/host/wayland_window.cc

Comment 9 by fangzhoug@chromium.org on Sun, Mar 13, 2022, 8:14 PM EDT

Status: Fixed (was: Assigned)

Comment 10 by sheriffbot on Wed, Mar 16, 2022, 12:42 PM EDT

Labels: reward-topanel

Comment 11 Deleted

Comment 12 by rzin...@gmail.com on Wed, Mar 16, 2022, 1:33 PM EDT

Regarding the severity mentioned in #C5: Need not necessarily be a custom build. It's possible to access with the flags --enable-features=UseOzonePlatform --ozone-platform=wayland.

Comment 13 by sheriffbot on Wed, Mar 16, 2022, 1:42 PM EDT

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

Comment 14 by amyressler@chromium.org on Thu, Apr 14, 2022, 5:00 PM EDT

Labels: -Security_Severity-Low Security_Severity-Medium based on the does not need a custom build to run/exploit, and is only behind a command line flag, adjusting severity accordingly

Comment 15 by wfh@chromium.org on Thu, Apr 14, 2022, 5:01 PM EDT

[VRP panel] hi fangzhoug has the variant analysis been performed as suggested in #3?

Also, is it possible to file a new issue to create a bot to run wayland tests under asan to try and shake out these bugs going forward? Thanks

Comment 16 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 PM EDT

Labels: -reward-topanel reward-unpaid reward-7000

*** 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 17 by sheriffbot on Fri, Apr 15, 2022, 1:17 PM EDT

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 18 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:58 PM EDT

Congratulations, Sri! The VRP Panel has decided to award you $7,000 for this report. Thank you for your efforts and reporting this interesting finding to us!

Comment 19 by rzin...@gmail.com on Fri, Apr 15, 2022, 3:42 PM EDT

Thank you Amy and VRP Panel ! This amount is equivalent to 1 meal/day for 108 people for a period of 21 years in our community. Thanks a lot !

Comment 20 by amyressler@google.com on Fri, Apr 15, 2022, 9:57 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 21 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:06 PM EDT

Labels: Release-0-M101

Comment 22 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT

Labels: CVE-2022-1487 CVE_description-missing

Comment 23 by fangzhoug@chromium.org on Fri, Apr 29, 2022, 2:52 PM EDT

We currently don't have a CI/CQ bot running run wayland tests under asan linux build. Filed crbug.com/1321215

Comment 24 by sheriffbot on Mon, Jun 20, 2022, 1:30 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 25 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 26 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing