☆ Starred by 3 users

Owner:	jarin@chromium.org
CC:	yuhengh@chromium.org weili@chromium.org yangguo@chromium.org ricea@chromium.org homi@chromium.org osh...@chromium.org dsv@google.com
Status:	Fixed *(Closed)*
Components:	Platform>DevTools
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Reward-1000
Needs-Feedback
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-97
FoundIn-86
external_security_report
M-98
Target-98
Security_Impact-Extended
Release-0-M101
CVE-2022-1493

Issue 1275414: Security: heap-use-after-free in network::server::HttpServer::FindConnection

Reported by hacky...@gmail.com on Wed, Dec 1, 2021, 12:22 AM EST

Code

VULNERABILITY DETAILS

[0] UiDevToolsServer class owns network::server::HttpServer,when UiDevToolsServer destroy,the server_ ptr will delete
https://source.chromium.org/chromium/chromium/src/+/main:components/ui_devtools/devtools_server.h;l=111

[1] And then UAF in HttpServer::FindConnection
https://source.chromium.org/chromium/chromium/src/+/main:services/network/public/cpp/server/http_server.cc;l=525

reproduce step
1. open chrome://inspect
2. click Inspect Native UI and then close this page
3. UAF occurs

```
=================================================================
==11772==ERROR: AddressSanitizer: heap-use-after-free on address 0x1200fb18cf78 at pc 0x7fff96c98e21 bp
0x007a1f3fc9a0 sp 0x007a1f3fc9e8
READ of size 8 at 0x1200fb18cf78 thread T0
    #0 0x7fff96c98e20 in network::server::HttpServer::FindConnection
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:525
    #1 0x7fff96c995a4 in network::server::HttpServer::OnWritable
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:350
    #2 0x7fffbb2045bb in mojo::SimpleWatcher::OnHandleReady
E:\src\chromium\src\mojo\public\cpp\system\simple_watcher.cc:278
    #3 0x7fff98966b04 in base::TaskAnnotator::RunTaskImpl E:\src\chromium\src\base\task\common\task_annotator.cc:135
    #4 0x7fff989b19b9 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #5 0x7fff989b1088 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #6 0x7fff98aabac6 in base::MessagePumpForUI::DoRunLoop
E:\src\chromium\src\base\message_loop\message_pump_win.cc:220
    #7 0x7fff98aa957f in base::MessagePumpWin::Run E:\src\chromium\src\base\message_loop\message_pump_win.cc:78
    #8 0x7fff989b3137 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #9 0x7fff988b1f43 in base::RunLoop::Run E:\src\chromium\src\base\run_loop.cc:140
    #10 0x7fff6b6b1aeb in content::BrowserMainLoop::RunMainMessageLoop
E:\src\chromium\src\content\browser\browser_main_loop.cc:1001
    #11 0x7fff6b6b7923 in content::BrowserMainRunnerImpl::Run
E:\src\chromium\src\content\browser\browser_main_runner_impl.cc:153
    #12 0x7fff6b6ab43f in content::BrowserMain E:\src\chromium\src\content\browser\browser_main.cc:30
    #13 0x7fff6d7f020e in content::RunBrowserProcessMain
E:\src\chromium\src\content\app\content_main_runner_impl.cc:646
    #14 0x7fff6d7f33c1 in content::ContentMainRunnerImpl::RunBrowser
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1159
    #15 0x7fff6d7f24f1 in content::ContentMainRunnerImpl::Run

E:\src\chromium\src\content\app\content_main_runner_impl.cc:1026
    #16 0x7fff6d7ee29f in content::RunContentProcess E:\src\chromium\src\content\app\content_main.cc:398
    #17 0x7fff6d7ef307 in content::ContentMain E:\src\chromium\src\content\app\content_main.cc:426
    #17 0x7fff6d7ef307 in content::ContentMain E:\src\chromium\src\content\app\content_main.cc:426
    #18 0x7fff703714a5 in ChromeMain E:\src\chromium\src\chrome\app\chrome_main.cc:172
    #19 0x7ff66c6b5544 in MainDllLoader::Launch E:\src\chromium\src\chrome\app\main_dll_loader_win.cc:169
    #20 0x7ff66c6b2a02 in main E:\src\chromium\src\chrome\app\chrome_exe_main_win.cc:382
    #21 0x7ff66c8864ab in __scrt_common_main_seh
D:\agent\_work\13\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #22 0x7fffe5be7033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #23 0x7fffe7a22650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

0x1200fb18cf78 is located 72 bytes inside of 104-byte region [0x1200fb18cf30,0x1200fb18cf98)
freed by thread T0 here:
    #0 0x7fffa934e46b in operator delete+0x8b (E:\src\chromium\src\out\Default\clang_rt.asan_dynamic-
x86_64.dll+0x18003e46b)
    #1 0x7fff666becb0 in ui_devtools::UiDevToolsServer::~UiDevToolsServer
E:\src\chromium\src\components\ui_devtools\devtools_server.cc:83
    #2 0x7fff666c1deb in ui_devtools::UiDevToolsServer::~UiDevToolsServer
E:\src\chromium\src\components\ui_devtools\devtools_server.cc:81
    #3 0x7fff666c1cf4 in ui_devtools::UiDevToolsServer::OnClose
E:\src\chromium\src\components\ui_devtools\devtools_server.cc:245
    #4 0x7fff96c9a19b in network::server::HttpServer::Close
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:160
    #5 0x7fff96c9c00d in network::server::HttpServer::HandleReadResult
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:277
    #6 0x7fff96c9b088 in network::server::HttpServer::OnReadable
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:257
    #7 0x7fffbb2045bb in mojo::SimpleWatcher::OnHandleReady
E:\src\chromium\src\mojo\public\cpp\system\simple_watcher.cc:278
    #8 0x7fff98966b04 in base::TaskAnnotator::RunTaskImpl E:\src\chromium\src\base\task\common\task_annotator.cc:135
    #9 0x7fff989b19b9 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #10 0x7fff989b1088 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #11 0x7fff98aabac6 in base::MessagePumpForUI::DoRunLoop
E:\src\chromium\src\base\message_loop\message_pump_win.cc:220
    #12 0x7fff98aa957f in base::MessagePumpWin::Run E:\src\chromium\src\base\message_loop\message_pump_win.cc:78
    #13 0x7fff989b3137 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #14 0x7fff988b1f43 in base::RunLoop::Run E:\src\chromium\src\base\run_loop.cc:140
    #15 0x7fff6b6b1aeb in content::BrowserMainLoop::RunMainMessageLoop
E:\src\chromium\src\content\browser\browser_main_loop.cc:1001
    #16 0x7fff6b6b7923 in content::BrowserMainRunnerImpl::Run
E:\src\chromium\src\content\browser\browser_main_runner_impl.cc:153
    #17 0x7fff6b6ab43f in content::BrowserMain E:\src\chromium\src\content\browser\browser_main.cc:30
    #18 0x7fff6d7f020e in content::RunBrowserProcessMain
E:\src\chromium\src\content\app\content_main_runner_impl.cc:646
    #19 0x7fff6d7f33c1 in content::ContentMainRunnerImpl::RunBrowser
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1159
    #20 0x7fff6d7f24f1 in content::ContentMainRunnerImpl::Run
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1026
    #21 0x7fff6d7ee29f in content::RunContentProcess E:\src\chromium\src\content\app\content_main.cc:398
    #22 0x7fff6d7ef307 in content::ContentMain E:\src\chromium\src\content\app\content_main.cc:426

    #23 0x7fff703714a5 in ChromeMain E:\src\chromium\src\chrome\app\chrome_main.cc:172
    #24 0x7ff66c6b5544 in MainDllLoader::Launch E:\src\chromium\src\chrome\app\main_dll_loader_win.cc:169
    #25 0x7ff66c6b2a02 in main E:\src\chromium\src\chrome\app\chrome_exe_main_win.cc:382
    #25 0x7ff66c6b2a02 in main E:\src\chromium\src\chrome\app\chrome_exe_main_win.cc:382
    #26 0x7ff66c8864ab in __scrt_common_main_seh
D:\agent\_work\13\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #27 0x7fffe5be7033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)

previously allocated by thread T0 here:
    #0 0x7fffa934e17b in operator new+0x8b (E:\src\chromium\src\out\Default\clang_rt.asan_dynamic-
x86_64.dll+0x18003e17b)
    #1 0x7fff666bf8d9 in ui_devtools::UiDevToolsServer::MakeServer
E:\src\chromium\src\components\ui_devtools\devtools_server.cc:180
    #2 0x7fff666c2fd5 in base::internal::Invoker<base::internal::BindState<void (ui_devtools::UiDevToolsServer::*)
(mojo::PendingRemote<network::mojom::TCPServerSocket>, int, const absl::optional<net::IPEndPoint>
&),base::WeakPtr<ui_devtools::UiDevToolsServer>,mojo::PendingRemote<network::mojom::TCPServerSocket> >,void (int,
const absl::optional<net::IPEndPoint> &)>::RunOnce E:\src\chromium\src\base\bind_internal.h:741
    #3 0x7fff706b572b in network::mojom::NetworkContext_CreateTCPServerSocket_ForwardToCallback::Accept
E:\src\chromium\src\out\Default\gen\services\network\public\mojom\network_context.mojom.cc:11024
    #4 0x7fffb9b59884 in mojo::InterfaceEndpointClient::HandleValidatedMessage
E:\src\chromium\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:895
    #5 0x7fffb9b69a88 in mojo::MessageDispatcher::Accept
E:\src\chromium\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #6 0x7fffb9b5d3c4 in mojo::InterfaceEndpointClient::HandleIncomingMessage
E:\src\chromium\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:657
    #7 0x7fffb9b76b4c in mojo::internal::MultiplexRouter::ProcessIncomingMessage
E:\src\chromium\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:1104
    #8 0x7fffb9b758e5 in mojo::internal::MultiplexRouter::Accept
E:\src\chromium\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:724
    #9 0x7fffb9b69a88 in mojo::MessageDispatcher::Accept
E:\src\chromium\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #10 0x7fffb9b49a91 in mojo::Connector::DispatchMessageW
E:\src\chromium\src\mojo\public\cpp\bindings\lib\connector.cc:556
    #11 0x7fffb9b4b584 in mojo::Connector::ReadAllAvailableMessages
E:\src\chromium\src\mojo\public\cpp\bindings\lib\connector.cc:614
    #12 0x7fffbb2045bb in mojo::SimpleWatcher::OnHandleReady
E:\src\chromium\src\mojo\public\cpp\system\simple_watcher.cc:278
    #13 0x7fff98966b04 in base::TaskAnnotator::RunTaskImpl E:\src\chromium\src\base\task\common\task_annotator.cc:135
    #14 0x7fff989b19b9 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #15 0x7fff989b1088 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #16 0x7fff98aabac6 in base::MessagePumpForUI::DoRunLoop
E:\src\chromium\src\base\message_loop\message_pump_win.cc:220
    #17 0x7fff98aa957f in base::MessagePumpWin::Run E:\src\chromium\src\base\message_loop\message_pump_win.cc:78
    #18 0x7fff989b3137 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
E:\src\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #19 0x7fff988b1f43 in base::RunLoop::Run E:\src\chromium\src\base\run_loop.cc:140
    #20 0x7fff6b6b1aeb in content::BrowserMainLoop::RunMainMessageLoop
E:\src\chromium\src\content\browser\browser_main_loop.cc:1001
    #21 0x7fff6b6b7923 in content::BrowserMainRunnerImpl::Run
E:\src\chromium\src\content\browser\browser_main_runner_impl.cc:153
    #22 0x7fff6b6ab43f in content::BrowserMain E:\src\chromium\src\content\browser\browser_main.cc:30
    #23 0x7fff6d7f020e in content::RunBrowserProcessMain

E:\src\chromium\src\content\app\content_main_runner_impl.cc:646
    #24 0x7fff6d7f33c1 in content::ContentMainRunnerImpl::RunBrowser
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1159
```

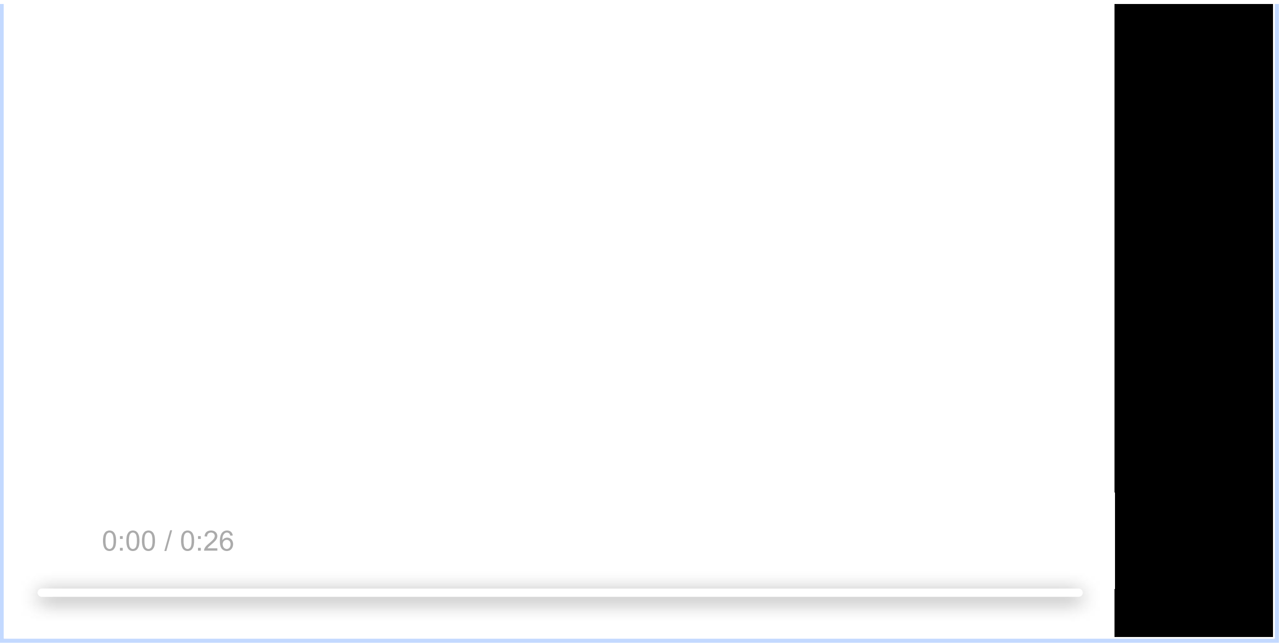
```
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1159
    #25 0x7fff6d7f24f1 in content::ContentMainRunnerImpl::Run
E:\src\chromium\src\content\app\content_main_runner_impl.cc:1026
    #26 0x7fff6d7ee29f in content::RunContentProcess E:\src\chromium\src\content\app\content_main.cc:398
    #27 0x7fff6d7ef307 in content::ContentMain E:\src\chromium\src\content\app\content_main.cc:426

SUMMARY: AddressSanitizer: heap-use-after-free
E:\src\chromium\src\services\network\public\cpp\server\http_server.cc:525 in network::server::HttpServer::FindConnection
Shadow bytes around the buggy address:
  0x042b1a631990: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x042b1a6319a0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x042b1a6319b0: fd fd fa fa fa fa fa fa fa fa fd fd fd fd fd fd
  0x042b1a6319c0: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x042b1a6319d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa
=>0x042b1a6319e0: fa fa fa fa fa fa fd fd fd fd fd fd fd fd fd[fd]
  0x042b1a6319f0: fd fd fd fa fa fa fa fa fa fa fa fa fd fd fd fd
  0x042b1a631a00: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x042b1a631a10: fa fa fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042b1a631a20: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x042b1a631a30: fd fd fd fd fd fd fa fa fa fa fa fa fa fa 00 00
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
==11772==ABORTING
```

VERSION
Chrome Version: 98.0.4738.0 dev x64
Operating System: 21h1

Reporter credit: Zhihua Yao of Kunlun Lab

2021-12-01 13-18-40.mp4
8.0 MB View Download

[redacted]



Comment 1 by sheriffbot on Wed, Dec 1, 2021, 12:31 AM EST

Labels: external_security_report

Comment 2 by hacky...@gmail.com on Wed, Dec 1, 2021, 7:17 AM EST

It’s really weird, I can’t reproduce it now, but I’m analyzing it in detail now

InspectMessageHandler::HandleLaunchUIDevToolsCommand [0] will set on_session_ended_ callback function to DestroyUiDevTools,when close [2],call the callback function [1] will reset devtools_server_,then UiDevToolsServer class owns network::server::HttpServer,when UiDevToolsServer destroy,the server_[3] ptr will be deleted,Eventually UAF happens [4]

```
void InspectMessageHandler::HandleLaunchUIDevToolsCommand(
    const base::ListValue* args) {
  // Start the UI DevTools server if needed and launch the front-end.
  if (!ChromeBrowserMainExtraPartsViews::Get()->GetUiDevToolsServerInstance()) {
    ChromeBrowserMainExtraPartsViews::Get()->CreateUiDevTools();

    // Make the server only lasts for a session.
    const ui_devtools::UiDevToolsServer* server =
        ChromeBrowserMainExtraPartsViews::Get()->GetUiDevToolsServerInstance();
    server->SetOnSessionEnded(base::BindOnce([]() {
      if (ChromeBrowserMainExtraPartsViews::Get()
              ->GetUiDevToolsServerInstance())
        ChromeBrowserMainExtraPartsViews::Get()->DestroyUiDevTools();  [0] //
    }));
  }
......

void UiDevToolsServer::SetOnSessionEnded(base::OnceClosure callback) const {
  on_session_ended_ = std::move(callback);
}
```

```
---------------------------------

void ChromeBrowserMainExtraPartsViews::DestroyUiDevTools() {
  devtools_process_observer_.reset();
  devtools_server_.reset();  [1] // std::unique_ptr<ui_devtools::UiDevToolsServer> devtools_server_;
}
---------------------------------

void UiDevToolsServer::OnClose(int connection_id) {
  DCHECK_CALLED_ON_VALID_SEQUENCE(devtools_server_sequence_);
  auto it = connections_.find(connection_id);
  if (it == connections_.end())
    return;
  UiDevToolsClient* client = it->second;
  client->Disconnect();
  connections_.erase(it);

  if (connections_.empty() && on_session_ended_)
    std::move(on_session_ended_).Run();  [2]
}
---------------------------------
```

[2] https://source.chromium.org/chromium/chromium/src/+/main:components/ui_devtools/devtools_server.h;l=111

```
---------------------------------
HttpConnection* HttpServer::FindConnection(int connection_id) {
  auto it = id_to_connection_.find(connection_id);
  if (it == id_to_connection_.end())
    return nullptr;
  return it->second.get();
} [4] //UAF
```

Comment 3 by jdeblasio@chromium.org on Wed, Dec 1, 2021, 8:38 PM EST

Status: Assigned (was: Unconfirmed)
Owner: yangguo@google.com
Labels: Needs-Feedback FoundIn-86 OS-Windows
Components: Platform>DevTools

This seems like a UAF, but I'm not sure how one could exploit this practically speaking. hackyzh002@: can you propose a plausible scenario on how an attacker could use this?

yangguo@: can you take a look at this, feeling free to re-assign as needed?

Comment 4 by sheriffbot on Wed, Dec 1, 2021, 8:39 PM EST

Labels: Security_Impact-Extended

Comment 5 by hacky...@gmail.com on Wed, Dec 1, 2021, 9:00 PM EST

Sorry jdeblasio@, at present, I don’t know how to exploit this kind of interaction, because I don’t know whether it can be triggered by other methods, such as javascript API, because I am not very familiar with this. You can refer to ~~Issue 1232628~~ and ~~Issue 1232617~~. At present, there are more UAFs of this kind.

Comment 6 by hacky...@gmail.com on Wed, Dec 1, 2021, 11:50 PM EST

If you want to reproduce this bug, you need to enable the Debugging tools for UI in chrome://flags/

Comment 7 by yangguo@google.com on Thu, Dec 2, 2021, 2:30 AM EST

Owner: osh...@chromium.org

Cc: homi@chromium.org yangguo@chromium.org

The DevTools team does not actually maintain UI DevTools, which is an alternate implementation of the backend, for Chrome UI.

Oshima, could you find an owner for this?

Comment 8 by jdeblasio@chromium.org on Thu, Dec 2, 2021, 8:11 PM EST

Labels: Security_Severity-Medium

I'm tentatively assigning security labels as a very heavily mitigated UAF in the browser process out of an abundance of caution, but it might not be a security bug at all. It should hopefully be a pretty straightforward fix once we find the correct owners, however, so oshima@, your help would be very appreciated. Thanks!

Comment 9 by sheriffbot on Fri, Dec 3, 2021, 12:52 PM EST

Labels: Target-97 M-97

Setting milestone and target because of medium severity.

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

Comment 10 by sheriffbot on Fri, Dec 3, 2021, 1:18 PM EST

Labels: -Pri-3 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 11 by osh...@chromium.org on Mon, Dec 6, 2021, 2:01 AM EST

Owner: weili@chromium.org

UI Devtools is available for aura/views platform, not just for chromeos. (and this is reported on Windows) Assigning weili@ who is one of owners of ui devtools in chrome team.

Comment 12 by sheriffbot on Thu, Dec 16, 2021, 12:21 PM EST

weili: Uh oh! This issue still open and hasn't been updated in the last 15 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 13 Deleted

Comment 14 by sheriffbot on Fri, Dec 31, 2021, 12:21 PM EST

weili: Uh oh! This issue still open and hasn't been updated in the last 30 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 15 by hacky...@gmail.com on Fri, Jan 7, 2022, 3:20 AM EST

So is this owner still on holiday?

Comment 16 by cthomp@chromium.org on Wed, Jan 12, 2022, 12:11 PM EST

Cc: ricea@chromium.org yuhengh@chromium.org weili@chromium.org

~~Issue 1282735~~ has been merged into this issue.

Comment 17 by cthomp@chromium.org on Wed, Jan 12, 2022, 12:12 PM EST

Owner: yuhengh@chromium.org

yuhengh@ could you take this bug following your investigation on ~~Issue 1282735~~?

+ricea@ who is owner for net/server/ code -- could you advise how DevTools code should destroy an HttpServer instance? Thanks!

Comment 18 by ricea@chromium.org on Wed, Jan 12, 2022, 11:14 PM EST

This seems to be the //services/network/public/cpp/server version of HttpServer, not the //net/server version, although they're almost identical. The way it's currently implemented makes it difficult to tear down safely. Possibly we could modify it to track connections that are currently pending deletion and have a method that deletes the server after all active connections are gone.

Comment 19 by sheriffbot on Wed, Feb 2, 2022, 12:21 PM EST

Labels: -M-97 M-98 Target-98

Comment 20 by yuhengh@chromium.org on Mon, Feb 7, 2022, 12:31 PM EST

Owner: weili@chromium.org

Not sure what's the best way to fix this, reassigning to code owner

Comment 21 by hacky...@gmail.com on Sun, Feb 13, 2022, 9:52 PM EST

hello,the code owner looks like no longer on chrome

Comment 22 by ricea@chromium.org on Mon, Feb 14, 2022, 3:20 AM EST

Status: Untriaged (was: Assigned)
Owner: ----

Sending for re-triage.

Comment 23 by hacky...@gmail.com on Tue, Feb 22, 2022, 8:37 PM EST

So someone reassign the owner?

Comment 24 by yangguo@google.com on Wed, Feb 23, 2022, 2:52 AM EST

Cc: osh...@chromium.org

Comment 25 by hacky...@gmail.com on Mon, Mar 7, 2022, 3:47 AM EST

```
--- chrome_browser_main_extra_parts_views.cc   2022-03-07 16:39:43.395067000 +0800
+++ chrome_browser_main_extra_parts_views_bak.cc 2022-03-07 16:39:43.395067000 +0800
@@ -208,5 +208,5 @@ ChromeBrowserMainExtraPartsViews::GetUiD

 void ChromeBrowserMainExtraPartsViews::DestroyUiDevTools() {
   devtools_process_observer_.reset();
-  devtools_server_.reset();
+  //devtools_server_.reset();
 }
```

With this patch, UAF will not happen

Comment 26 by ricea@chromium.org on Mon, Mar 7, 2022, 7:31 AM EST

#25 Doesn't this just create a memory leak? It's not clear to me that it won't just move the UAF somewhere else, either.

Comment 27 by hacky...@gmail.com on Mon, Mar 7, 2022, 7:43 AM EST

Maybe there will be a memory leak, the best way is to use weakptr

Comment 28 by jarin@chromium.org on Mon, Mar 7, 2022, 8:29 AM EST

Owner: jarin@chromium.org

Comment 29 by sheriffbot on Mon, Mar 7, 2022, 2:23 PM EST

Status: Assigned (was: Untriaged)

Comment 30 by jarin@chromium.org on Tue, Mar 8, 2022, 8:25 AM EST

hackyzh002@, do you have some reproduction instructions? I cannot even see the flags in chrome://flags on Linux or Windows (it looks like it might be ChromeOS-only - https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/about_flags.cc;l=4626;drc=97c2dc1068cf2a2f7eb95a128542bf7b064172de).

Comment 31 Deleted

Comment 32 Deleted

Comment 33 by hacky...@gmail.com on Tue, Mar 8, 2022, 8:40 AM EST

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/about_flags.cc;l=7426

```
    "ui-debug-tools"
```

ui-debug-tools

Comment 34 by jarin@chromium.org on Tue, Mar 8, 2022, 9:10 AM EST

Thanks, that worked - I can now inspect. However, still no UAF (I tried both asan release and asan debug).

Comment 35 by yuhengh@chromium.org on Tue, Mar 8, 2022, 11:15 AM EST

FYI, it's easier to reproduce on Mac
~~https://crbug.com/1282735#c6~~

Comment 36 by jarin@chromium.org on Tue, Mar 8, 2022, 11:43 AM EST

I do not have a Mac, but I do have an idea for a fix. It would be great if someone could try out(?)

Here is the CL: https://chromium-review.googlesource.com/c/chromium/src/+/3510307

Comment 37 by Git Watcher on Wed, Mar 9, 2022, 4:21 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/8ef4631cac23a205c0d237c087dba82674f1ce6e

commit 8ef4631cac23a205c0d237c087dba82674f1ce6e
Author: Jaroslav Sevcik <jarin@chromium.org>
Date: Wed Mar 09 09:20:01 2022

Use weak pointers for devtools http server handlers

This makes sure that we do not call HttpServer message handlers
on a deallocated HttpServer instance.

Interestingly, the weak pointer factory was already there, but
it was unused.

~~Bug: chromium:1275414~~
Change-Id: Ic0c33319bb3e67e3c15349d07acbaad64a7f62e3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3510307
Reviewed-by: Robbie McElrath <rmcelrath@chromium.org>
Reviewed-by: Danil Somsikov <dsv@chromium.org>
Commit-Queue: Jaroslav Sevcik <jarin@chromium.org>
Cr-Commit-Position: refs/heads/main@{#979140}

[modify]
https://crrev.com/8ef4631cac23a205c0d237c087dba82674f1ce6e/services/network/public/cpp/server/http_server.cc

Comment 38 by hacky...@gmail.com on Thu, Mar 10, 2022, 2:59 PM EST

This is fixed!Please change the status

Comment 39 by jarin@google.com on Fri, Mar 11, 2022, 4:00 PM EST

Status: Fixed (was: Assigned)

Comment 40 by sheriffbot on Sat, Mar 12, 2022, 12:41 PM EST

Labels: reward-topanel

Comment 41 by sheriffbot on Sat, Mar 12, 2022, 1:40 PM EST

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

Comment 42 by amyressler@google.com on Wed, Mar 16, 2022, 9:46 PM EDT

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 43 by amyressler@chromium.org on Wed, Mar 16, 2022, 10:31 PM EDT

Hello, the VRP Panel has decided to award you $1,000 for this report. While we appreciate you efforts, we understand this reward amount may be less than you expected. The reasons for this reward judgement are:
1) there was no demonstrated exploitability or explanation how an attacker would leverage this bug
2) the direct access and user interaction with dev tools required to trigger this issue
3) the lack of reliability to reasonably trigger this issue

Comment 44 by hacky...@gmail.com on Wed, Mar 16, 2022, 10:39 PM EDT

Hello,this vulnerability attack is also relatively simple. The victim directly accesses devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=127.0.0.1:9223/0, and then closes the tab page to trigger this vulnerability. I think it is necessary to Raise the bounty for this bug

Comment 45 by hacky...@gmail.com on Wed, Mar 16, 2022, 10:42 PM EDT

And you can see this microsoft's attack scenarios for devtools. https://microsoftedge.github.io/edgevr/posts/attacking-the-devtools/

Comment 46 by jarin@chromium.org on Thu, Mar 17, 2022, 2:38 AM EDT

Re #43, additionally, the attacker would need to activate the "ui-debug-tools" experimental flag (which is off by default).

Comment 47 by amyressler@chromium.org on Thu, Mar 17, 2022, 4:17 PM EDT

hello, as expressed in comment #43- yes, "relatively simple" in terms of steps, however, not as simple in comparison to exploitation via remote content or a single click remote POC, as this requires direct UI access to dev tools and convincing a user to engage in these steps for an attacker to leverage this bug.

I will still run it back by the panel for reconsideration, however, as conveyed in previous comms and the email to the researcher community about the updates to our rules and policies [1]:
"There is a recent trend of reports away from issues triggered by remote content to issues that are strongly or solely dependent on user interaction. While we appreciate your efforts to discover and report these bugs, these issues are not as impactful or exploitable as those that demonstrate exploitability through remote content.

The amounts listed are for good quality reports that don't require complex or unlikely user interaction. Reports of issues that rely heavily or solely on user interaction, instead of being triggered by remote content, will generally receive significantly reduced rewards. Less convincing or more constrained bug submissions will likely qualify for reduced reward amounts, as

reduced rewards. Less convincing or more constrained bug submissions will likely qualify for reduced reward amounts, as chosen at the discretion of the reward panel.
Reports of issues that involve implausible interaction, interactions a user would not be realistically convinced to perform, may not be rewarded."

[1] https://g.co/chrome/vrp

Comment 48 by hacky...@gmail.com on Thu, Mar 17, 2022, 8:52 PM EDT

Yes. But the bounty is unreasonable, I think it is very likely to dampen the research enthusiasm of researchers

Comment 49 by amyressler@chromium.org on Wed, Mar 23, 2022, 3:45 PM EDT

Hello, the VRP Panel has decided that the award amount is sufficient for this issue as conveyed by this report. As mentioned in comments #43 and comment #47, if you are able to provide a demonstration of exploitability via remote content or and not requiring direct user interaction via dev tools, we are happy to reassess this issue and the reward amount.

Comment 50 by amyressler@google.com on Fri, Mar 25, 2022, 5:23 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 51 by amyressler@chromium.org on Mon, Apr 25, 2022, 8:57 PM EDT

Labels: Release-0-M101

Comment 52 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT

Labels: CVE-2022-1493 CVE_description-missing

Comment 53 by sheriffbot on Sat, Jun 18, 2022, 1:31 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 54 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 55 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing