[chromium](#) ▾[New issue](#)




Open issues ▾



Search chromium issue ▾

[Sign in](#)

☆ Starred by 4 users

Owner: lgrey@chromium.org
OOO until Dec 1**CC:** sadrul@chromium.org
 nmehta@google.com
 dsv@google.com**Status:**Fixed (*Closed*)**Components:**[Platform](#)>[DevTools](#)**Modified:**

Jul 29, 2022

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:[Linux](#), [Windows](#), [Mac](#)**Pri:**

2

Type:[Bug-Security](#)[reward-2000](#)[Security_Severity-Low](#)[allpublic](#)[reward-inprocess](#)[CVE_description-submitted](#)[external_security_report](#)[FoundIn-100](#)[Security_Impact-Extended](#)[Release-0-M102](#)[CVE-2022-1876](#)

Issue 1313600: Security: heap-buffer-overflow on components/ui_devtools/views/devtools_server_util.cc

Reported by [rheza...@gmail.com](#) on Tue, Apr 5, 2022, 4:15 PM EDT

 Code

VULNERABILITY DETAILS

Similar with [issue #1313574](#)

VERSION

Chrome Version: 102.0.4987.0 + dev

Operating System: linux-chromeOS and Linux

REPRODUCTION CASE

Option 1

1. Open browser and navigate to devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=localhost:9222/1 while issue # devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=localhost:9222/0

Option 2

1. Install plugin

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

```
=====
==87795==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60900171c448 at pc 0x561f90c3db40 bp
0x7fff53251ed0 sp 0x7fff53251ec8
READ of size 8 at 0x60900171c448 thread T0 (chrome)
SCARINESS: 23 (8-byte-read-heap-buffer-overflow)
#0 0x561f90c3db3f in get buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:288:19
#1 0x561f90c3db3f in ui_devtools::UiDevToolsServer::OnWebSocketRequest(int, network::server::HttpServerRequestInfo
const&) components/ui_devtools/devtools_server.cc:218:50
#2 0x561f90c42f40 in network::server::HttpServer::HandleReadResult(network::server::HttpConnection*, unsigned int)
services/network/public/cpp/server/http_server.cc:309:18
#3 0x561f90c41ed0 in network::server::HttpServer::OnReadable(int, unsigned int, mojo::HandleSignalsState const&)
services/network/public/cpp/server/http_server.cc:257:3
#4 0x561f90c464c3 in Invoke<void (network::server::HttpServer::*)(int, unsigned int, const mojo::HandleSignalsState &),
const base::WeakPtr<network::server::HttpServer> &, const int &, unsigned int, const mojo::HandleSignalsState &>
base/bind_internal.h:542:12
#5 0x561f90c464c3 in MakeItSo<void (network::server::HttpServer::*const &)(int, unsigned int, const
mojo::HandleSignalsState &), const base::WeakPtr<network::server::HttpServer> &, const int &, unsigned int, const
mojo::HandleSignalsState &> base/bind_internal.h:726:5
#6 0x561f90c464c3 in RunImpl<void (network::server::HttpServer::*const &)(int, unsigned int, const
mojo::HandleSignalsState &), const std::__1::tuple<base::WeakPtr<network::server::HttpServer>, int> &, 0UL, 1UL>
base/bind_internal.h:779:12
#7 0x561f90c464c3 in base::internal::Invoker<base::internal::BindState<void (network::server::HttpServer::*)(int, unsigned
int, mojo::HandleSignalsState const&), base::WeakPtr<network::server::HttpServer>, int>, void (unsigned int,
mojo::HandleSignalsState const&)>::Run(base::internal::BindStateBase*, unsigned int, mojo::HandleSignalsState const&)
```

```

base/bind_internal.h:761:12
#8 0x561f894066d7 in Run base/callback.h:241:12
#9 0x561f894066d7 in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&)
mojo/public/cpp/system/simple_watcher.cc:278:14
#10 0x561f8940769f in Invoke<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &),
base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState> base/bind_internal.h:542:12
#11 0x561f8940769f in MakeItSo<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &),
base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState> base/bind_internal.h:726:5
#12 0x561f8940769f in RunImpl<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &),
std::__1::tuple<base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>, 0UL, 1UL, 2UL, 3UL>
base/bind_internal.h:779:12
#13 0x561f8940769f in base::internal::Invoker<base::internal::BindState<void (mojo::SimpleWatcher::*)(int, unsigned int,
mojo::HandleSignalsState const&), base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>,
void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:748:12
#14 0x561f888adb93 in Run base/callback.h:142:12
#15 0x561f888adb93 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
base/task/common/task_annotator.cc:135:32
#16 0x561f888efecd in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:388:29)>
base/task/common/task_annotator.h:74:5
#17 0x561f888efecd in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:386:21
#18 0x561f888ef5c4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:291:41
#19 0x561f888f0bb1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
#20 0x561f887a60c9 in HandleDispatch base/message_loop/message_pump_glib.cc:375:46
#21 0x561f887a60c9 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*)
base/message_loop/message_pump_glib.cc:126:43
#0 0x7f2e3cde517c in g_main_context_dispatch ??:0:0

```

0x60900171c448 is located 0 bytes to the right of 8-byte region [0x60900171c440,0x60900171c448)
allocated by thread T0 (chrome) here:

```

#0 0x561f7990e91d 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 0x561f90c3e7c5 in __libcpp_operator_new<unsigned long> buildtools/third_party/libc++/trunk/include/new:235:10
#2 0x561f90c3e7c5 in __libcpp_allocate buildtools/third_party/libc++/trunk/include/new:261:10
#3 0x561f90c3e7c5 in allocate buildtools/third_party/libc++/trunk/include/__memory/allocator.h:82:38
#4 0x561f90c3e7c5 in allocate buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:261:20
#5 0x561f90c3e7c5 in __split_buffer buildtools/third_party/libc++/trunk/include/__split_buffer:314:29
#6 0x561f90c3e7c5 in void std::__1::vector<std::__1::unique_ptr<ui_devtools::UiDevToolsClient,
std::__1::default_delete<ui_devtools::UiDevToolsClient> >,
std::__1::allocator<std::__1::unique_ptr<ui_devtools::UiDevToolsClient,
std::__1::default_delete<ui_devtools::UiDevToolsClient> > >
>::__push_back_slow_path<std::__1::unique_ptr<ui_devtools::UiDevToolsClient,
std::__1::default_delete<ui_devtools::UiDevToolsClient> > >(std::__1::unique_ptr<ui_devtools::UiDevToolsClient,
std::__1::default_delete<ui_devtools::UiDevToolsClient> >&&) buildtools/third_party/libc++/trunk/include/vector:1625:49
#7 0x561f90c3ce44 in push_back buildtools/third_party/libc++/trunk/include/vector:1657:9
#8 0x561f90c3ce44 in ui_devtools::UiDevToolsServer::AttachClient(std::__1::unique_ptr<ui_devtools::UiDevToolsClient,
std::__1::default_delete<ui_devtools::UiDevToolsClient> >) components/ui_devtools/devtools_server.cc:161:12
#9 0x561f826289b4 in ui_devtools::CreateUiDevToolsServerForViews(network::mojom::NetworkContext*,
std::__1::unique_ptr<ui_devtools::ConnectorDelegate, std::__1::default_delete<ui_devtools::ConnectorDelegate> >

```

```

std::__1::unique_ptr<ui_devtools::ConnectorDelegate, std::__1::default_delete<ui_devtools::ConnectorDelegate> >,
base::FilePath const&) components/ui_devtools/views/devtools_server_util.cc:42:11
#10 0x561f93b0d050 in ChromeBrowserMainExtraPartsViews::CreateUiDevTools()
chrome/browser/ui/views/chrome_browser_main_extra_parts_views.cc:197:22
#11 0x561f93b0cc6d in ChromeBrowserMainExtraPartsViews::PreProfileInit()
chrome/browser/ui/views/chrome_browser_main_extra_parts_views.cc:121:5
#12 0x561f8783534e in ChromeBrowserMainParts::PreProfileInit() chrome/browser/chrome_browser_main.cc:1168:24
#13 0x561f883afe13 in ChromeBrowserMainPartsLinux::PreProfileInit()
chrome/browser/chrome_browser_main_linux.cc:103:32
#14 0x561f878338f7 in ChromeBrowserMainParts::PreMainMessageLoopRunImpl()
chrome/browser/chrome_browser_main.cc:1544:3
#15 0x561f87832f04 in ChromeBrowserMainParts::PreMainMessageLoopRun()
chrome/browser/chrome_browser_main.cc:1142:18
#16 0x561f7ee959aa in content::BrowserMainLoop::PreMainMessageLoopRun()
content/browser/browser_main_loop.cc:983:28
#17 0x561f8005f008 in Run base/callback.h:142:12
#18 0x561f8005f008 in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:43:29
#19 0x561f7ee94f2d in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:894:25
#20 0x561f7ee9bbb1 in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams)
content/browser/browser_main_runner_impl.cc:134:15
#21 0x561f7ee917ce in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:26:32
#22 0x561f8764acc0 in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:640:10
#23 0x561f8764e1ec in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
content/app/content_main_runner_impl.cc:1147:10
#24 0x561f8764d517 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1019:12
#25 0x561f87646d31 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content/app/content_main.cc:407:36
#26 0x561f8764745c in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:435:10
#27 0x561f79911126 in ChromeMain chrome/app/chrome_main.cc:176:12
#28 0x7f2e3b89a0b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-start.c:308:16

```

SUMMARY: AddressSanitizer: heap-buffer-overflow

buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:288:19 in get

Shadow bytes around the buggy address:

```

0x0c12802db830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c12802db840: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c12802db850: fa fa 00 fa fa fa fa fa fa fa fa fa fa fa fa
0x0c12802db860: fa fa fa fa 00 fa fa fa fa fa fa fa fa fa fa
0x0c12802db870: fa fa fa fa fa fa 00 fa fa fa fa fa fa fa fa
=>0x0c12802db880: fa fa fa fa fa fa fa fa 00[fa]fa fa fa fa fa
0x0c12802db890: fa fa fa fa fa fa fa fa fa 00 00 fa fa fa fa
0x0c12802db8a0: fa fa fa fa fa fa fa fa fa fa fa fa 04 fa fa
0x0c12802db8b0: fa fa fa fa fa fa fa fa fa fa fa fa fa 00 fa
0x0c12802db8c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c12802db8d0: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

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 right redzone: t3
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
==87795==ABORTING

[Comment 1](#) by [sheriffbot](#) on Tue, Apr 5, 2022, 4:16 PM EDT Project Member

Labels: external_security_report

[Comment 2](#) by [rheza...@gmail.com](#) on Tue, Apr 5, 2022, 4:18 PM EDT

Sorry missing arguments:

Needing --enable-ui-devtools=9222 enable.

background.js

129 bytes [View](#) [Download](#)

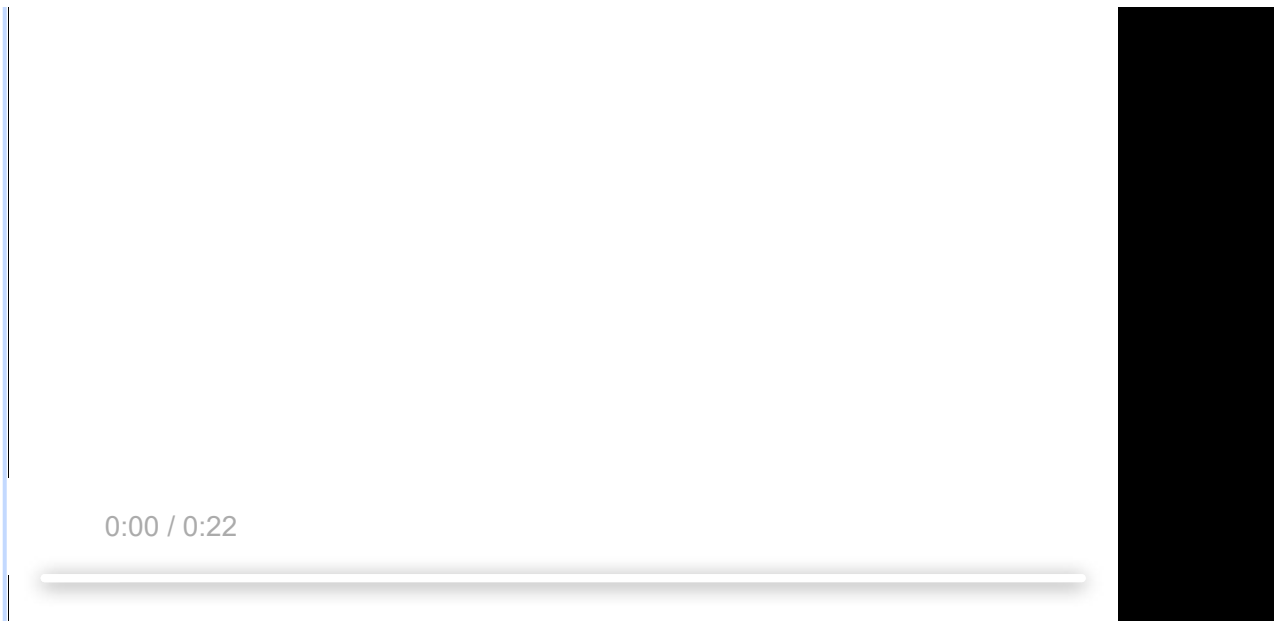
manifest.json

339 bytes [View](#) [Download](#)

[Deleted] **screencast_1313600_plugin.webm**

screencast_1313600.webm

2.3 MB [View](#) [Download](#)



Comment 3 by [rheza...@gmail.com](#) on Tue, Apr 5, 2022, 4:20 PM EDT

oops clarify the repro:

Option 1

1. Open browser and navigate to `devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=localhost:9222/1` while [issue #1313574](#) "devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=localhost:9222/0"

Option 2

1. Install plugin

Comment 4 by [rsesek@chromium.org](#) on Wed, Apr 6, 2022, 5:36 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: lgrey@chromium.org

Cc: sadrul@chromium.org

Labels: Security_Severity-Low FoundIn-100 Security_Impact-Stable OS-Linux OS-Mac OS-Windows Pri-2

Components: Platform>DevTools

Thanks, I can confirm this. Steps that reproed for me are:

1. Launch with `--enable-ui-devtools=9222`
2. Navigate to `devtools://devtools/bundled/devtools_app.html?uiDevTools=true&ws=localhost:9222/1`

`connection_id` is not validated here before indexing the array:

https://source.chromium.org/chromium/chromium/src/+main:components/ui_devtools/devtools_server.cc;l=218;drc=729f2502700cbb51589fd7a2bff221663035293e

Because this requires the developer option `--enable-ui-devtools`, this is Low.

bug-1313600.txt

10.6 KB [View](#) [Download](#)

Comment 5 by [sheriffbot](#) on Wed, Apr 6, 2022, 5:41 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 6 by [Git Watcher](#) on Mon, Apr 11, 2022, 6:53 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+2039b7264b8d1c653d4ef876aa1aa221fb98ad7e>

commit [2039b7264b8d1c653d4ef876aa1aa221fb98ad7e](#)

Author: Leonard Grey <lgrey@chromium.org>

Date: Mon Apr 11 22:52:50 2022

UIDevTools: Fix server test on Mac

(Though TBH I couldn't get it to pass locally on Linux either!)

Not *directly* related to <https://crbug.com/1313600> but I want the tests in good shape so that fix can have a test. This is in a separate change for better revertability/granularity.

~~Bug: 1313600~~

Change-Id: I8d9e22312c9911b5470619f18603022f3b4c6a2d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3577365>

Reviewed-by: Robert Sesek <rsesek@chromium.org>

Commit-Queue: Leonard Grey <lgrey@chromium.org>

Cr-Commit-Position: refs/heads/main@{#991248}

[modify] https://crrev.com/2039b7264b8d1c653d4ef876aa1aa221fb98ad7e/components/ui_devtools/devtools_server.cc

[modify]

https://crrev.com/2039b7264b8d1c653d4ef876aa1aa221fb98ad7e/components/ui_devtools/devtools_server_unittest.cc

[modify] https://crrev.com/2039b7264b8d1c653d4ef876aa1aa221fb98ad7e/components/ui_devtools/devtools_server.h

Comment 7 by [Git Watcher](#) on Tue, Apr 12, 2022, 7:15 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+6bbdbf771fc7ff458724de4720154123b2dd019>

commit [6bbdbf771fc7ff458724de4720154123b2dd019](#)

Author: Leonard Grey <lgrey@chromium.org>

Date: Tue Apr 12 23:14:06 2022

UIDevTools: fix bounds check for websocket connections

~~Bug: 1313600~~

Change-Id: Ic97da6e5cf5595d530a100bc8bbbee12467cef05

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3584284>

Reviewed-by: Robert Sesek <rsesek@chromium.org>

Commit-Queue: Leonard Grey <lgrey@chromium.org>

Cr-Commit-Position: refs/heads/main@{#991786}

[modify] https://crrev.com/6bbdbf771fc7ff458724de4720154123b2dd019/components/ui_devtools/devtools_server.cc

[modify]

https://crrev.com/6bbdbf771fc7ff458724de4720154123b2dd019/components/ui_devtools/devtools_server_unittest.cc

Comment 8 by lgrey@chromium.org on Mon, Apr 18, 2022, 10:20 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 9 by [sheriffbot](#) on Mon, Apr 18, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 10 by [sheriffbot](#) on Mon, Apr 18, 2022, 1:41 PM EDT Project Member

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

Comment 11 by [amyressler@chromium.org](#) on Mon, May 23, 2022, 9:49 PM EDT Project Member

Labels: Release-0-M102

Comment 12 by [amyressler@google.com](#) on Tue, May 24, 2022, 2:17 PM EDT Project Member

Labels: CVE-2022-1876 CVE_description-missing

Comment 13 by [amyressler@chromium.org](#) on Thu, Jul 21, 2022, 2:45 PM EDT Project Member

Cc: nmehta@google.com

Comment 14 by [sheriffbot](#) on Mon, Jul 25, 2022, 1:31 PM EDT Project Member

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 15 by [amyressler@google.com](#) on Wed, Jul 27, 2022, 5:26 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 16 by [amyressler@google.com](#) on Thu, Jul 28, 2022, 7:38 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-2000

*** 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.

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)

Comment 17 by [amyressler@chromium.org](#) on Thu, Jul 28, 2022, 8:13 PM EDT Project Member

Congratulations, Rhea! The VRP Panel has decided to award you \$2,000 for this report. The reward amount decided up was based on this issue being significantly mitigated by not being remote exploitable, requiring developers option/ high

amount of user interaction required, and requiring an extension to be installed. Thank you for your efforts and reporting this issue to us.

[Comment 18](#) by amyressler@chromium.org on Thu, Jul 28, 2022, 8:13 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

[Comment 19](#) by amyressler@google.com on Fri, Jul 29, 2022, 7:52 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess