☆ Starred by 4 users

Owner:	a...@chromium.org
CC:	maxlg@google.com a...@chromium.org smcgruer@chromium.org rouslan@chromium.org maxlg@chromium.org lukasza@chromium.org mea...@chromium.org tommi@chromium.org mgiuca@chromium.org mfoltz@chromium.org sergeyu@chromium.org jophba@chromium.org w...@chromium.org creis@chromium.org eladalon@chromium.org ellyj...@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Permissions>Prompts UI>Security>UrlFormatting UI>Browser>MediaCapture
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Lacros
Pri:	1
Type:	Bug-Security

reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-95
external_security_report
M-96
Target-96

FoundIn-94
Security_Impact-Extended
Release-0-M97

Issue 1255713: Security: UI spoofing using a very long URL

Reported by stw.s...@gmail.com on Mon, Oct 4, 2021, 12:07 PM EDT

Code

VULNERABILITY DETAILS
Changing the URL using `history.replaceState` to 10M+ characters causes a spoofing bug in various security UIs.

VERSION
Chrome Version: 94.0.4606.71 + all channels
Operating System: Tested on Windows 10, Mac OS, Android 11

REPRODUCTION CASE

# Classic Tab
1. Open https://example.com
2. Eval: `history.replaceState(null, '', window.location.pathname + '?' + 'x'.repeat(10000000));`
3. URL is `about:blank#blocked`

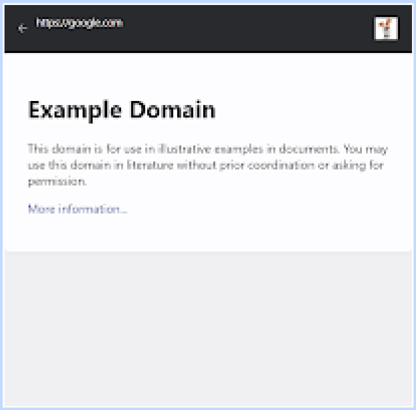
# Payment Dialog
1. Go to https://liquangumax.github.io/apps/max-nonbasiccard/ and Install
2. Go to https://maxlgu.github.io/pr/max-nonbasiccard/ and click Buy
3. Navigate the payment dialog to https://example.com
4. Eval: `history.replaceState(null, '', window.location.pathname + '?' + 'x'.repeat(10000000));`
5. URL is not displayed
6. (Optionally) change the title: `document.title='https:\u200e//google.com'`

# Screen Share Dialog
1. Open https://example.com
2. Eval: `history.replaceState(null, '', window.location.pathname + '?' + 'x'.repeat(10000000));`
3. Eval: `navigator.mediaDevices.getDisplayMedia()`
4. Page origin is not displayed in the dialog.

Attached are screenshots of the bug in various UIs.

CREDIT INFORMATION
Reporter credit: Thomas Orlita

payment-dialog-custom-title-spoof.png
25.9 KB View Download



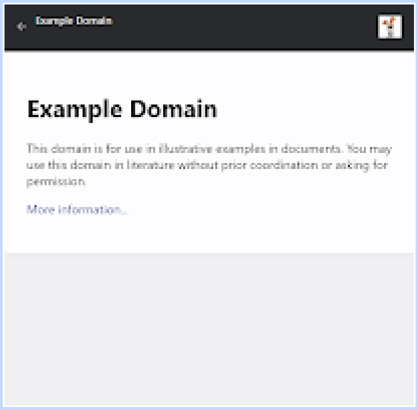
https://google.com

Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

payment-dialog-spoof.png
25.5 KB View Download



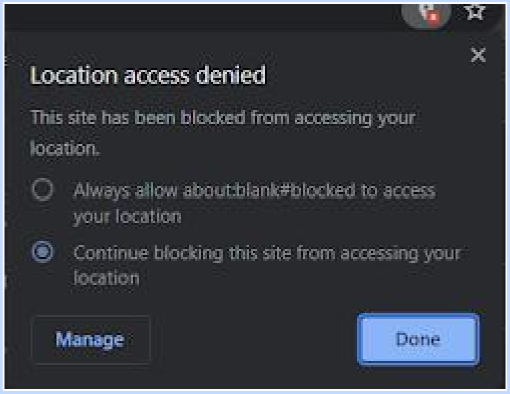
Example Domain

Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

permission-access-denied-spoof.png
16.9 KB View Download



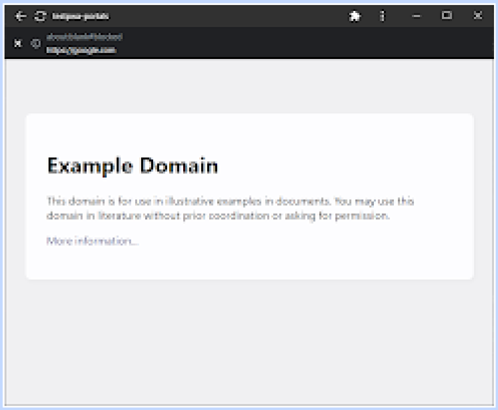
Location access denied

This site has been blocked from accessing your location.

○ Always allow about:blank#blocked to access your location

● Continue blocking this site from accessing your location

pwa-custom-title-spoof.png
28.6 KB View Download



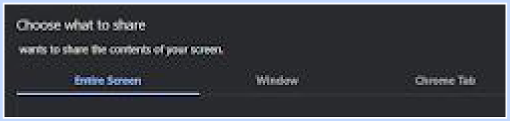
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

screen-share-dialog-spoof.png

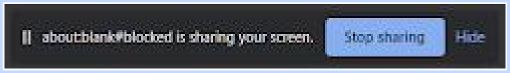
4.3 KB View Download


Choose what to share

wants to share the contents of your screen.

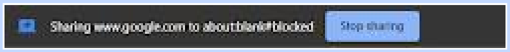
screen-share-fullscreen-share-spoof.png

4.7 KB View Download


about:blank#blocked is sharing your screen.

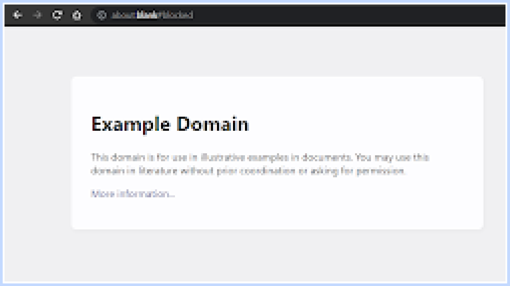
screen-share-tab-share-spoof.png

4.3 KB View Download


Sharing www.google.com to about:blank#blocked

tab-url-spoof.png

24.5 KB View Download



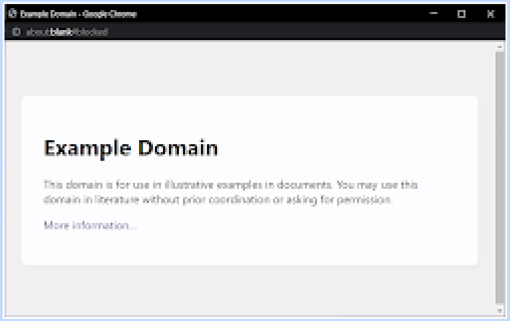
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

window-url-spoof.png

30.6 KB View Download



Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

Comment 1 by sheriffbot on Mon, Oct 4, 2021, 12:11 PM EDT Project Member

Labels: external_security_report

Comment 2 by rsleevi@chromium.org on Mon, Oct 4, 2021, 12:17 PM EDT Project Member

Labels: FoundIn-94 Security_Severity-Medium OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: UI>Security>UrlFormatting UI>Browser>Permissions>Prompts

Thanks for the great write-up!

I'm tentatively tagging this as Medium; it doesn't appear you're able to spoof the UI, so much as cause it to not display properly, but that still represents an interesting edge case here and definitely seems "tamper" worthy.

Comment 3 by rsleevi@chromium.org on Mon, Oct 4, 2021, 12:20 PM EDT Project Member

Owner: nasko@chromium.org

nasko: Could you help route this? Your name comes up from https://source.chromium.org/chromium/chromium/src/+/413468f8e2196ea59444399c517a3a6b72fa86c3 / ~~Issue 899788~~ , so I'm hoping you may have pointers or thoughts here.

Comment 4 by sheriffbot on Mon, Oct 4, 2021, 12:23 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 5 by sheriffbot on Mon, Oct 4, 2021, 12:52 PM EDT Project Member

Labels: Target-95 M-95

Setting milestone and target because of medium severity.

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

Comment 6 by sheriffbot on Mon, Oct 4, 2021, 2:17 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 7 by creis@chromium.org on Mon, Oct 4, 2021, 3:46 PM EDT Project Member

Cc: a...@chromium.org mea...@chromium.org lukasza@chromium.org
Components: Blink>Payments UI>Browser>MediaCapture

Thanks for the report. As comment 2 notes, this is more about causing a missing URL or a confusing "about:blank#blocked" URL to show in dialogs, rather than showing an attacker-controlled URL, but in some of the cases it still appears to be an issue in practice.

For this specific approach, maybe there's a way to enforce an identical length limit in the renderer process to avoid failing the FilterURL check, but I'm not sure if that would rule out all the ways FilterURL might rewrite it to about:blank#blocked.

More generally, dialogs probably need to be more robust to about:blank-like URLs (as discussed in ~~issue 1241497~~ and issue 1228702).

I don't think tab-url-spoof.png and window-url-spoof.png are significant concerns (since the attacker can't put a victim's URL in the address bar), but some of the other screenshots are concerning:
* payment-dialog-custom-title-spoof.png shows no URL, allowing the title to look like a URL. This is a problem.
* permission-access-denied-spoof.png is confusing if not necessarily dangerous?
* pwa-custom-title-spoof.png at least shows about:blank#blocked, but also allows an attacker-controlled title. Might be a problem.

* The screen-share images also show a missing and confusing URL.

Origin might be a better thing to display in all these cases? avi@ / meacer@: Do you have thoughts on how to address this more generally?

Comment 8 by nasko@chromium.org on Mon, Oct 4, 2021, 9:13 PM EDT Project Member

Owner: a...@chromium.org

Removing myself as the owner, since creis@ has triaged the bug. Assigning tentatively to avi@, who has been doing some work recently, though feel free to reassign to more appropriate person.

Comment 9 by a...@chromium.org on Fri, Oct 8, 2021, 2:53 PM EDT Project Member

I had raised the question of formatting URLs, but that doesn't quite make me someone who has been working on this recently :)

I'm in agreement with comment 7 by creis@. The "about:blank#blocked" ones don't worry me right now. The use of page-controlled titles do. I can bring this to the security UI folks; this seems like a pretty large question about what we want dialogs to look like.

Comment 10 by a...@chromium.org on Fri, Oct 8, 2021, 2:57 PM EDT Project Member

I see the point about the disappearing origins. Let me look into the URL formatters.

Comment 11 by a...@chromium.org on Fri, Oct 8, 2021, 3:06 PM EDT Project Member

We have too many functions for URL formatting (IMO) but I added printfs to them all and none appear to be called for these dialogs. This is concerning; let me dig further.

Comment 12 by a...@chromium.org on Fri, Oct 8, 2021, 3:41 PM EDT Project Member

For the screen sharing dialog, the string comes from DisplayMediaAccessHandler::ProcessQueuedAccessRequest() which tries to do the right thing but hits an antipattern.

They could have done:

```
  picker_params.app_name = url_formatter::FormatUrlForSecurityDisplay(
      web_contents->GetLastCommittedURL(),
      url_formatter::SchemeDisplay::OMIT_CRYPTOGRAPHIC);
```

which would say "about:blank#blocked wants to share the contents of your screen".

They could have done:

```
  picker_params.app_name = url_formatter::FormatOriginForSecurityDisplay(
      web_contents->GetMainFrame()->GetLastCommittedOrigin(),
      url_formatter::SchemeDisplay::OMIT_CRYPTOGRAPHIC);
```

which would correctly say "example.com wants to share the contents of your screen".

But they did:

```
 picker_params.app_name = url_formatter::FormatOriginForSecurityDisplay(
     url::Origin::Create(web_contents->GetLastCommittedURL()),
     url_formatter::SchemeDisplay::OMIT_CRYPTOGRAPHIC);
```

and url::Origin::Create() creates a null origin, which url_formatter::FormatOriginForSecurityDisplay turns into an empty string.

Issues here:
1. The fact that “about:blank#blocked” turns into a null Origin isn’t great.
2. `FormatOriginForSecurityDisplay` should probably hard-CHECK if a null Origin is passed to it.
3. Can we do anything about the antipattern of `url::Origin::Create(web_contents->GetLastCommittedURL())`?

Comment 13 by a...@chromium.org on Fri, Oct 8, 2021, 3:54 PM EDT Project Member

Specifically, the antipattern `url::Origin::Create(web_contents->GetLastCommittedURL())` allows a page to launder its origin into an opaque origin unrelated to its URL.

Comment 14 by a...@chromium.org on Fri, Oct 8, 2021, 3:58 PM EDT Project Member

https://source.chromium.org/search?q=Origin::Create.*LastCommittedURL&ss=chromium

It is used more often than it should.

Comment 15 by a...@chromium.org on Fri, Oct 8, 2021, 4:46 PM EDT Project Member

Cc: maxlg@google.com

Comment 16 by maxlg@google.com on Fri, Oct 8, 2021, 4:59 PM EDT Project Member

Cc: rouslan@chromium.org

Comment 17 by rouslan@chromium.org on Fri, Oct 8, 2021, 7:17 PM EDT Project Member

Cc: smcgruer@chromium.org

Comment 18 by a...@chromium.org on Sat, Oct 9, 2021, 3:17 PM EDT Project Member

I have https://crrev.com/c/3212580 for the media picker, and https://crrev.com/c/3213747 for the payment picker.

https://crrev.com/c/3213301 makes FormatOriginForSecurityDisplay CHECK for opaque origins, but that is very red for tests. I need to investigate.

The permissions prompts are probably failing due to using URLs rather than origins, but the problem is that Android doesn’t have Origin formatting like our C++ does.

Comment 19 by Git Watcher on Mon, Oct 11, 2021, 7:06 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07

commit 6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07
Author: Avi Drissman <avi@chromium.org>
Date: Mon Oct 11 23:05:56 2021

Add formatOriginForSecurityDisplay to Java

~~Bug: 1255713~~
Change-Id: I1ec7c6cb143342c12c31c6bb0d6872a12495fe4f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3216454
Reviewed-by: Ted Choc <tedchoc@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>

Cr-Commit-Position: refs/heads/main@{#930320}

[modify] https://crrev.com/6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07/components/url_formatter/BUILD.gn
[modify] https://crrev.com/6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07/components/url_formatter/android/BUILD.gn
[modify]
https://crrev.com/6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07/components/url_formatter/android/java/src/org/chromium/components/url_formatter/UrlFormatter.java
[modify]
https://crrev.com/6ae36cd32eb7c21fa2a5d4761e37ea5c272adf07/components/url_formatter/url_formatter_android.cc

Comment 20 by a...@chromium.org on Wed, Oct 13, 2021, 12:22 AM EDT Project Member

I have fixes for payments and screen sharing in the works. The PWA issue is in CustomTabBarView::UpdateContents() and right now it seems beyond my ability to easily fix.

Comment 21 by Git Watcher on Wed, Oct 13, 2021, 12:37 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/84ce1c7414d2d7fce208787f34fedd75a083973e

commit 84ce1c7414d2d7fce208787f34fedd75a083973e
Author: Avi Drissman <avi@chromium.org>
Date: Wed Oct 13 16:36:13 2021

Correctly use FormatOriginForSecurityDisplay in the media access dialog callers

For the display of an origin, FormatOriginForSecurityDisplay is the
correct function to use. Ensure that it is used and used correctly
by the callers of DesktopMediaPicker::Show(), and in other places
where the origin of a tab needs to be displayed.

~~Bug: 1255713~~
Change-Id: Iec98e2be6a995fe59c6376516330fa84cb6b8ce4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3212580
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#931084}

[modify]
https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/ui/views/tab_sharing/tab_sharing_ui_views.cc
[modify]
https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/ui/tab_sharing/tab_sharing_infobar_delegate_unittest.cc
[modify]
https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/ui/tab_sharing/tab_sharing_infobar_delegate.cc
[modify]
https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/media/webrtc/desktop_capture_access_handler.cc
[modify]
https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/media/webrtc/display_media_access_handler.cc
[modify]

https://crrev.com/84ce1c7414d2d7fce208787f34fedd75a083973e/chrome/browser/ui/views/tab_sharing/tab_sharing_ui_views_browsertest.cc

Comment 22 by Git Watcher on Wed, Oct 13, 2021, 2:53 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b0eb49065f24771bf42e534e7be00c958799f27a

commit b0eb49065f24771bf42e534e7be00c958799f27a
Author: Avi Drissman <avi@chromium.org>
Date: Wed Oct 13 18:51:41 2021

Use FormatOriginForSecurityDisplay in the payment dialog

~~Bug: 1255713~~
Change-Id: I173a767c5902939c2c7031049c32eec573f2a095
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3213747
Reviewed-by: Liquan (Max) Gu <maxlg@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#931164}

[modify]
https://crrev.com/b0eb49065f24771bf42e534e7be00c958799f27a/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 23 by a...@chromium.org on Wed, Oct 13, 2021, 3:00 PM EDT Project Member

Splitting the Origin antipattern to ~~issue 1259711~~.

Comment 24 by a...@chromium.org on Wed, Oct 13, 2021, 7:51 PM EDT Project Member

Media sharing is fixed. Payments on desktop is fixed, but payments on Android requires infrastructure for Java Origin that doesn’t yet exist and is being discussed. PWAs show URLs in CustomTabBarView::UpdateContents() but it shares a lot of infrastructure with the omnibox so it’s not clear to me how to fix it.

What else is there to do? Do we want to do a more thorough retrofit of Origin?

Comment 25 by mfoltz@chromium.org on Wed, Oct 13, 2021, 8:03 PM EDT Project Member

FWIW I have a patch up to fix the Cast dialog which should land soon. There may need to be a similar patch for Zenith, I haven't investigated yet.

Comment 26 by sheriffbot on Fri, Oct 29, 2021, 12:21 PM EDT Project Member

avi: 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 27 by a...@chromium.org on Fri, Oct 29, 2021, 1:08 PM EDT Project Member

What else can be done here?

The immediate issue of missing origins in the dialogs is fixed (at least on desktop). There remain underlying issues: That GURL.GetOrigin returns a GURL (though it’s been renamed), that Origin::Create is still problematic, that the Origin infrastructure on Android is underbuilt and some of the fixes on desktop cannot be made on Android until that happens.

Is this something that we need to assemble a task force to handle, or do we call this bug done?

Comment 28 by sheriffbot on Fri, Nov 12, 2021, 12:22 PM EST Project Member

avi: Uh oh! This issue still open and hasn't been updated in the last 14 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 29 by sheriffbot on Mon, Nov 15, 2021, 12:21 PM EST Project Member

Labels: -M-95 Target-96 M-96

Comment 30 by maxlg@google.com on Mon, Nov 15, 2021, 3:11 PM EST Project Member

Cc: maxlg@chromium.org

Comment 31 by smcgruer@chromium.org on Tue, Nov 16, 2021, 9:59 AM EST Project Member

Components: -Blink>Payments

Removing Blink>Payments as the payment-part is fixed (thanks avi@!) and this is tripping our SLO metrics for being an open P1 bug.

FWIW, I would agree with closing this as fixed given lack of apparent appetite to do the follow-throughs that you suggested; otherwise I expect it will just lie open forever :/.

Comment 32 by a...@chromium.org on Tue, Nov 16, 2021, 4:21 PM EST Project Member

Status: Fixed (was: Assigned)

Closing this now; the Origin work is being tracked in bug 1270878. Thanks, lukasza@!

Comment 33 by sheriffbot on Wed, Nov 17, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 34 by sheriffbot on Wed, Nov 17, 2021, 1:41 PM EST Project Member

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

Comment 35 by amyressler@google.com on Tue, Nov 23, 2021, 7:20 PM EST Project Member

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 36 by amyressler@chromium.org on Tue, Nov 23, 2021, 8:05 PM EST Project Member

Congratulations! The VRP Panel has decided to award you $3000 for this report. Please let us know what name or handle/pseudonym you would like used for acknowledgement of this issue in our release notes. Thank you for reporting this issue and nice work!

In the future, we kindly request that you please attach POCs and other files directly and individually to security bug reports (rather than linking or zip/compressed files).
Failure to do so may result in a slightly reduced reward amount. Thank you!!

Comment 37 by stw.s...@gmail.com on Wed, Nov 24, 2021, 6:33 AM EST

Hi Amy,
You can use "Thomas Orlita" as the name.
Thanks!

Comment 38 by amyressler@chromium.org on Wed, Nov 24, 2021, 10:01 AM EST Project Member

Thanks and thanks for providing it again! I completely missed that you provided that in the original report above.

Comment 39 by amyressler@chromium.org on Mon, Nov 29, 2021, 10:16 AM EST Project Member

Labels: -reward-unpaid reward-inprocess

was sent to finance for VRP reward payment processing on 24 November 2021

Comment 40 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:22 PM EST Project Member

Labels: Release-0-M97

Comment 41 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0112 CVE_description-missing

Comment 42 by sheriffbot on Thu, Feb 24, 2022, 1:30 PM EST 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 43 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted