☆ Starred by 23 users

Owner:	mahmadi@chromium.org
CC:	tommycli@chromium.org owone@chromium.org orinj@chromium.org jdonnelly@chromium.org mpear...@chromium.org mfacey@chromium.org yoangela@chromium.org manukh@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>NewTabPage
Modified:	Jun 27, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-94
M-94
FoundIn-93
LTS-Security-90
LTS-Security-NotApplicable-90
Security_Impact-Extended
merge-merged-4606
merge-merged-94
merge-merged-4638
merge-merged-95
merge-merged-4664
Merge-Merged-96
Release-1-M95
CVE-2021-37999

Issue 1251541: Security: Universal Cross-Site Scripting (UXSS) - completing previously searched text in NTP

Reported by ashis...@gmail.com on Tue, Sep 21, 2021, 5:15 AM EDT

Code

VULNERABILITY DETAILS:

Universal Cross-Site Scripting - UXSS is a type of attack that exploits client-side vulnerabilities in the browser or browser extensions in order to generate an XSS condition, and execute malicious code. When such vulnerabilities are found and exploited, the behavior of the browser is affected and its security features may be bypassed or disabled.

Chrome Version:

Version 93.0.4577.82 (Official Build)

Operating System:

Any OS with Google Chrome Browser installed.

Steps To Reproduce:

Step1: Create a HTML file - see xss.html

Step2: This file contains the CSRF code to search in Google search bar with XSS payload as - "><img src=x onerror=alert(1337)>

Step3: Send this File to Victim.

Step4: Once the request is submitted from CSRF attached html file.

Step5: It will create a search result in Google search bar

As soon as Victim goes to search bar to search anything XSS will get triggered.

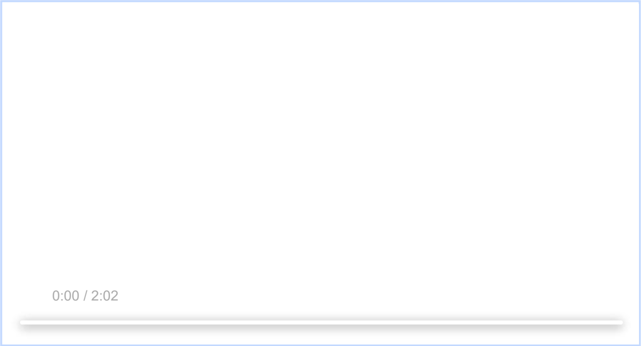
Request you to please go through my attached POC,

POC: https://drive.google.com/drive/folders/1PrQ1dP3JAWfkJMDqKTV6DJNoHaUlqabr?usp=sharing

Thank You
Ashish Arun Dhone

xss.html
1.5 KB View Download

Chrome_XSS_POC.mp4
3.7 MB View Download



Comment 1 by sheriffbot on Tue, Sep 21, 2021, 5:20 AM EDT Project Member

Labels: external_security_report

Comment 2 by ajgo@google.com on Tue, Sep 21, 2021, 3:30 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: mahmadi@chromium.org
Cc: tommycli@chromium.org jdonnelly@chromium.org manukh@chromium.org mpear...@chromium.org orinj@chromium.org yoangela@chromium.org
Labels: FoundIn-93 Security_Severity-High Pri-1
Components: UI>Browser>NewTabPage

Thanks - this repros:

1 - visit xss.html
2- click submit
3 - open the ntp
4 - click in the search box

(Anyone watching the video above might want to skip to the final 20s or so.)

Assigning based on realbox OWNERS - feel free to CC in more people or assign to someone else.

Comment 3 by sheriffbot on Tue, Sep 21, 2021, 3:30 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 4 by ajgo@google.com on Tue, Sep 21, 2021, 3:31 PM EDT Project Member

Summary: Security: Universal Cross-Site Scripting (UXSS) - completing previously searched text in NTP (was: Security: Universal Cross-Site Scripting (UXSS))

Comment 5 by ashis...@gmail.com on Wed, Sep 22, 2021, 1:52 AM EDT

Hello Team,

What I have observed is,

Say Victim is using "Laptop A" suppose victim open xss.html file --> click submit --> open the NTP --> Click in Search Box and XSS will get triggered.

Now if victim uses "Laptop B" and login with same Google account which he is using in "Laptop A" then victim just have to Click in Search Box and same XSS will get triggered irrespective of any system as this XSS payload is getting stored in history and this will create more impact.

Thank You!!

Comment 6 by sheriffbot on Wed, Sep 22, 2021, 12:51 PM EDT Project Member

Labels: Target-94 M-94

Setting milestone and target because of high severity.

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

Comment 7 by ajgo@google.com on Wed, Sep 22, 2021, 7:56 PM EDT Project Member

~~Issue 1252146~~ has been merged into this issue.

Comment 8 by mahmadi@chromium.org on Mon, Sep 27, 2021, 2:39 PM EDT Project Member

Status: Started (was: Assigned)

Comment 9 by ashis...@gmail.com on Mon, Sep 27, 2021, 2:47 PM EDT

Hello Team,

What does status: started means?

Comment 10 by ajgo@google.com on Mon, Sep 27, 2021, 3:43 PM EDT Project Member

~~Issue 1253217~~ has been merged into this issue.

Comment 11 by ajgo@google.com on Mon, Sep 27, 2021, 4:34 PM EDT Project Member

~~Issue 1253393~~ has been merged into this issue.

Comment 12 by ashis...@gmail.com on Sun, Oct 3, 2021, 2:08 PM EDT

Hello Team,

Hope you are doing well.
Any updates on this issue?

Thank you

Comment 13 by mahmadi@chromium.org on Mon, Oct 4, 2021, 11:46 AM EDT Project Member

Issue 1255238 has been merged into this issue.

Comment 14 by tsepez@chromium.org on Fri, Oct 8, 2021, 8:51 PM EDT Project Member

~~Issue 1258205~~ has been merged into this issue.

Comment 15 by tsepez@chromium.org on Fri, Oct 8, 2021, 8:53 PM EDT Project Member

~~Issue 1257997~~ has been merged into this issue.

Comment 16 by tsepez@chromium.org on Fri, Oct 8, 2021, 9:02 PM EDT Project Member

~~Issue 1256905~~ has been merged into this issue.

Comment 17 by xinghuilu@chromium.org on Mon, Oct 11, 2021, 8:16 PM EDT Project Member

~~Issue 1258809~~ has been merged into this issue.

Comment 18 by mahmadi@chromium.org on Mon, Oct 11, 2021, 9:09 PM EDT Project Member

This is resulting from the way the aria-label is computed by assigning the match content to a temporary element's innerHTML in [1] in order for the text content to be extracted. innerHTML renders the HTML markup allowing for any scripts in the match content to execute. Note that this does not happen with inner-h-t-m-l Polymer binding in [2] since the DOM being injected into has already been parsed.

I'm not 100% positive if match content can contain HTML markup (useful markup for styling and not XSS) and why the decision was made at the time to use innerHTML to sieve out the markup. A safer alternative to using innerHTML will be using textContent with the caveat that if the match content does contain markup those will appear in the value for the aria-label attr. I will send out this fix shortly.

The next step will be to verify if matches do not contain useful markup and whether this indirection can be avoided entirely.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/resources/new_tab_page/realbox/realbox_match.js;l=291,297;drc=e4dcd712f358ef167da95e0b960d3512a7896c8d
[2]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/resources/new_tab_page/realbox/realbox_match.html;l=111,113;drc=e4dcd712f358ef167da95e0b960d3512a7896c8d

Comment 19 by mahmadi@chromium.org on Mon, Oct 11, 2021, 9:09 PM EDT Project Member

Labels: OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros

Comment 20 by jdonnelly@chromium.org on Tue, Oct 12, 2021, 10:12 AM EDT Project Member

Cc: mfacey@chromium.org

Comment 21 by jdonnelly@chromium.org on Tue, Oct 12, 2021, 10:17 AM EDT Project Member

Should https://crrev.com/c/3218631 have a vague title to avoid revealing information about the attack before it's merged and distributed? Something like, "Change assignment of answer text" or the like?

Comment 22 by tsepez@chromium.org on Tue, Oct 12, 2021, 1:28 PM EDT Project Member

Re: c21, generally no, but since this isn't a traditional full-up XSS, we'd might like to change the title to be more accurate and avoid the term XSS. Maybe something like "assign to textContent in .. "

Comment 23 by tsepez@chromium.org on Tue, Oct 12, 2021, 1:54 PM EDT Project Member

BTW, I filed ~~https://crbug.com/1259251~~ as a follow-up. I failed to make this happen some years ago, so perhaps its time for someone to take another look.

Comment 24 by mahmadi@chromium.org on Tue, Oct 12, 2021, 2:45 PM EDT Project Member

I changed the title of the CL to something less conspicuous.

To add more context, the logic to sieve out HTML markup was added in crrev.com/c/2965565 in M93 when support for suggestion answers was added to the NTP realbox. Unfortunately the CL does not give much clue as to why the logic was added. I believe the assumption must have been that the suggestion answers may contain markup. I don't see any indication of that in [2]. Could any of the Omnibox owners here verify whether that could be the case?

[1] http://shortn/_JDLvGubpgX
[2] http://shortn/_1ONCU1Efun

Comment 25 by ashis...@gmail.com on Tue, Oct 12, 2021, 3:16 PM EDT

Hello All,

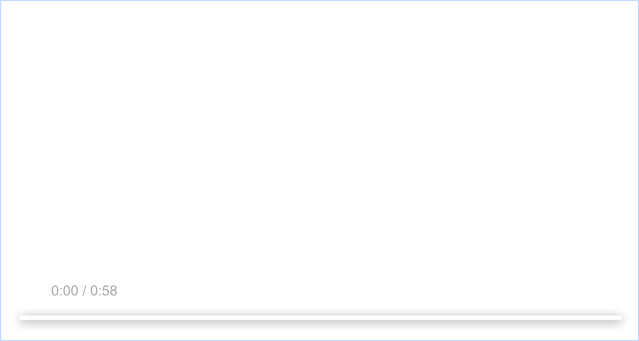
I don't know why subject is to be changed from XSS, it is JavaScript execution where I can actually execute scripts. As a result I am attaching a POC where we can redirect victim to any website and run scripts.

PFA of the html file and POC Video.

Thank You!!

xss.html
1.5 KB View Download

XSS-Redirect-POC.mp4
3.7 MB View Download



Comment 26 by bdea@chromium.org on Tue, Oct 12, 2021, 3:43 PM EDT Project Member

~~Issue 1259299~~ has been merged into this issue.

Comment 27 by mahmadi@chromium.org on Tue, Oct 12, 2021, 4:03 PM EDT Project Member

follow up to #26, looking at the other other entry points, Omnibox in [1] and CrOS app list in [2], the *additional text* of the answer's first line is being appended to the match contents if one exists and second line of the answer is used as is as the description which is consistent with what the Realbox does in [3]. I couldn't find any indication that the additional text of the answer's first line contains any of its own markup. I think we should continue using that on the JS side as if it's just text and take advantage the client-side generated markup for the match contents to render it. Note that the match content is a prefix of the answer's first line the way it's implemented in the realbox, thus the match contents markup will be compatible with it.

[1] http://shortn/_QmF48SHHGm
[2] http://shortn/_Kf7doqIMaY
[3] http://shortn/_7F7QmUm0of

Comment 28 by mahmadi@chromium.org on Tue, Oct 12, 2021, 5:06 PM EDT Project Member
Cc: owone@chromium.org

Comment 29 by Git Watcher on Tue, Oct 12, 2021, 8:52 PM EDT Project Member
Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/10939d3c6653ef2cc8105bb4145db6a876c22e61

commit 10939d3c6653ef2cc8105bb4145db6a876c22e61
Author: Moe Ahmadi <mahmadi@chromium.org>
Date: Wed Oct 13 00:51:56 2021

[realbox] Treat suggestion answers as text without HTML markup

The current implementation assumes that suggestion answers contain HTML markup and accounts for that when generating the a11y label for the match. This is expensive and may expose security vulnerabilities. This CL changes that assumption and treats the suggestion answers as text without HTML markup.

This CL also makes sure that the client-side generated markup for the match contents is used to render the suggestion answers. Note that the match contents is a prefix of the answer's first line. Therefore the match contents markup is applicable to the answer's first line.

For more info see ~~crbug.com/1251541~~

~~Fixed: 1251541~~
Change-Id: I7352301c672691dd97681eed480f22f738f21ae9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3218631
Commit-Queue: Moe Ahmadi <mahmadi@chromium.org>
Auto-Submit: Moe Ahmadi <mahmadi@chromium.org>
Reviewed-by: Justin Donnelly <jdonnelly@chromium.org>
Reviewed-by: dpapad <dpapad@chromium.org>
Cr-Commit-Position: refs/heads/main@{#930882}

[modify] https://crrev.com/10939d3c6653ef2cc8105bb4145db6a876c22e61/chrome/browser/resources/new_tab_page/realbox/realbox_match.js

Comment 30 by sheriffbot on Wed, Oct 13, 2021, 12:42 PM EDT Project Member
Labels: reward-topanel

Comment 31 by sheriffbot on Wed, Oct 13, 2021, 1:41 PM EDT Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 32 by sheriffbot on Wed, Oct 13, 2021, 2:01 PM EDT Project Member
Labels: Merge-Request-96 Merge-Request-94 Merge-Request-95

Requesting merge to stable M94 because latest trunk commit (930882) appears to be after stable branch point (911515).

Requesting merge to beta M95 because latest trunk commit (930882) appears to be after beta branch point (920003).

Requesting merge to dev M96 because latest trunk commit (930882) appears to be after dev branch point (929512).

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

Comment 33 by sheriffbot on Wed, Oct 13, 2021, 8:53 PM EDT Project Member
Labels: -Merge-Request-96 Merge-Approved-96 Hotlist-Merge-Approved

Merge approved: your change passed merge requirements and is auto-approved for M96. Please go ahead and merge the CL to branch 4664 (refs/branch-heads/4664) manually. Please contact milestone owner if you have questions.
Merge instructions: https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 34 by sheriffbot on Wed, Oct 13, 2021, 8:53 PM EDT Project Member
Labels: -Merge-Request-95 Merge-Review-95 Hotlist-Merge-Review

Merge review required: M95 has already been cut for stable release.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative? https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), None (ChromeOS), pbommana (Desktop)

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

Comment 35 by sheriffbot on Wed, Oct 13, 2021, 8:53 PM EDT Project Member
Labels: -Merge-Request-94 Merge-Review-94

Merge review required: M94 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines

2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative? https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 36 by ashis...@gmail.com on Wed, Oct 13, 2021, 9:16 PM EDT

Hello Team,
Hope you are doing well!!

Any updates on reward and CVE?

Comment 37 by mahmadi@chromium.org on Thu, Oct 14, 2021, 12:15 PM EDT Project Member

Status: Verified (was: Fixed)

1. Why does your merge fit within the merge criteria for these milestones? Security fixes
2. What changes specifically would you like to merge? crrev.com/c/3218631
3. Have the changes been released and tested on canary? Verified the fix in Canary Desktop 97.0.4669.0 on Mac.
4. Is this a new feature? No
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? The change has already been verified. For additional verification please follow the steps below:
a) search for <img src=x onerror=alert(1337)> in the Omnibox or the NTP Realbox.
b) click into the NTP Realbox (you may need to click into the realbox twice) until <img src=x onerror=alert(1337)> shows as a zero-prefix suggestion.
c) in the milestones which do not include the fix an alert popup will open once the suggestion shows in the NTP realbox. In the milestones which do include the fix an alert popup does not open.

Comment 38 by amyressler@chromium.org on Thu, Oct 14, 2021, 3:54 PM EDT Project Member

since this fix just landed less than 24 hours ago, I'm going to defer approving for merge for now to allow for some more thorough bake time on Canary; Stable RC for M95 has already been cut so this can be included first stable respin for M95

Comment 39 by amyressler@chromium.org on Thu, Oct 14, 2021, 3:59 PM EDT Project Member

to answer comment #36: hello, Ashish and thanks for your questions. Once a security bug is fixed it gets updated with the reward-topanel label so it can be included in the VRP Panel discussions for consideration for a potential VRP reward.
Since this just happened less than 24 hours ago, it missed the cutoff for this week's panel discussion so it will be up considered during a forthcoming panel discussion.

CVE IDs are issued at the time the fix goes into release; as I mentioned in comment #38, this missed the cutoff for M95 so it should be included in the first security refresh for M95, which is scheduled to for release on 2 November. A CVE will be applied to this issue that day.

Comment 40 by ashis...@gmail.com on Thu, Oct 14, 2021, 10:27 PM EDT

To answer Comment #39:
Thanks for the detailed explanation :)

Comment 41 by srinivassista@google.com on Fri, Oct 15, 2021, 12:40 PM EDT Project Member

This issue has been approved for Merge to M96, Please help complete your merges no later than 12pm PST (Monday Oct 18) so that they can go out in next week beta promotion build. I would like to get beta coverage for these CL's as much as we can .

Comment 42 by bdea@chromium.org on Fri, Oct 15, 2021, 2:58 PM EDT Project Member

~~Issue 1260222~~ has been merged into this issue.

Comment 43 by sheriffbot on Mon, Oct 18, 2021, 12:13 PM EDT Project Member

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 44 by srinivassista@google.com on Mon, Oct 18, 2021, 1:13 PM EDT Project Member

Pls complete the merges to M96 branch asap. I am cutting the RC build for dev release (which will be promoted to beta) today at 3pm PST, pls complete all merges before 3pm PST today (Monday Oct 18, 2021)

Comment 45 by Git Watcher on Tue, Oct 19, 2021, 2:11 PM EDT Project Member

Status: Fixed (was: Verified)
Labels: -merge-approved-96 merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/60ce07072e343e9dcef5e3ee244bc13b641dcc9f

commit 60ce07072e343e9dcef5e3ee244bc13b641dcc9f
Author: Moe Ahmadi <mahmadi@chromium.org>
Date: Tue Oct 19 18:10:43 2021

[M96][realbox] Treat suggestion answers as text without HTML markup

The current implementation assumes that suggestion answers contain HTML
markup and accounts for that when generating the a11y label for the
match. This is expensive and may expose security vulnerabilities. This
CL changes that assumption and treats the suggestion answers as text
without HTML markup.

This CL also makes sure that the client-side generated markup for the
match contents is used to render the suggestion answers. Note that the
match contents is a prefix of the answer's first line. Therefore the
match contents markup is applicable to the answer's first line.

For more info see ~~crbug.com/1251541~~

(cherry picked from commit 10939d3c6653ef2cc8105bb4145db6a876c22e61)

~~Fixed: 1251541~~
Change-Id: I7352301c672691dd97681eed480f22f738f21ae9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3218631
Commit-Queue: Moe Ahmadi <mahmadi@chromium.org>
Auto-Submit: Moe Ahmadi <mahmadi@chromium.org>

Reviewed-by: Justin Donnelly <jdonnelly@chromium.org>
Reviewed-by: dpapad <dpapad@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#930882}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3229677
Cr-Commit-Position: refs/branch-heads/4664@{#218}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/60ce07072e343e9dcef5e3ee244bc13b641dcc9f/chrome/browser/resources/new_tab_page/realbox/realbox_match.js

Comment 46 by amyressler@chromium.org on Tue, Oct 19, 2021, 2:27 PM EDT Project Member
Labels: -Merge-Review-95 Merge-Approved-95 Merge-Approved-94

Now that this has had sufficient time on Canary, as long as there are no issues or concerns with stability, please go ahead and merge to M95, branch 4638, at your earliest convenience so this can be included in the first security refresh for M95.

Additionally, if possible, please merge to M94, branch 4606, so this fix can be included in the Extended Stable security refresh.

Comment 47 by amyressler@chromium.org on Tue, Oct 19, 2021, 3:44 PM EDT Project Member
Labels: -Merge-Review-94

Comment 48 by Git Watcher on Tue, Oct 19, 2021, 8:35 PM EDT Project Member
Labels: -merge-approved-94 merge-merged-4606 merge-merged-94

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0acea24516305427f2dcad85b98e6faf6f3e8908

commit 0acea24516305427f2dcad85b98e6faf6f3e8908
Author: Moe Ahmadi <mahmadi@chromium.org>
Date: Wed Oct 20 00:34:33 2021

[M94][realbox] Treat suggestion answers as text without HTML markup

The current implementation assumes that suggestion answers contain HTML
markup and accounts for that when generating the a11y label for the
match. This is expensive and may expose security vulnerabilities. This
CL changes that assumption and treats the suggestion answers as text
without HTML markup.

This CL also makes sure that the client-side generated markup for the
match contents is used to render the suggestion answers. Note that the
match contents is a prefix of the answer's first line. Therefore the
match contents markup is applicable to the answer's first line.

For more info see ~~crbug.com/1251541~~

(cherry picked from commit 10939d3c6653ef2cc8105bb4145db6a876c22e61)

~~Fixed: 1251541~~
Change-Id: I7352301c672691dd97681eed480f22f738f21ae9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3218631
Commit-Queue: Moe Ahmadi <mahmadi@chromium.org>
Auto-Submit: Moe Ahmadi <mahmadi@chromium.org>
Reviewed-by: Justin Donnelly <jdonnelly@chromium.org>
Reviewed-by: dpapad <dpapad@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#930882}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3232359
Cr-Commit-Position: refs/branch-heads/4606@{#1380}
Cr-Branched-From: 35b0d5a9dc8362adfd44e2614f0d5b7402ef63d0-refs/heads/master@{#911515}

[modify] https://crrev.com/0acea24516305427f2dcad85b98e6faf6f3e8908/chrome/browser/resources/new_tab_page/realbox/realbox_match.js

Comment 49 by Git Watcher on Tue, Oct 19, 2021, 8:42 PM EDT Project Member
Labels: -merge-approved-95 merge-merged-4638 merge-merged-95

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7095119c76ff55ed7e1706f6728cd98476e69f98

commit 7095119c76ff55ed7e1706f6728cd98476e69f98
Author: Moe Ahmadi <mahmadi@chromium.org>
Date: Wed Oct 20 00:41:16 2021

[M95][realbox] Treat suggestion answers as text without HTML markup

The current implementation assumes that suggestion answers contain HTML
markup and accounts for that when generating the a11y label for the
match. This is expensive and may expose security vulnerabilities. This
CL changes that assumption and treats the suggestion answers as text
without HTML markup.

This CL also makes sure that the client-side generated markup for the
match contents is used to render the suggestion answers. Note that the
match contents is a prefix of the answer's first line. Therefore the
match contents markup is applicable to the answer's first line.

For more info see ~~crbug.com/1251541~~

(cherry picked from commit 10939d3c6653ef2cc8105bb4145db6a876c22e61)

~~Fixed: 1251541~~
Change-Id: I7352301c672691dd97681eed480f22f738f21ae9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3218631
Commit-Queue: Moe Ahmadi <mahmadi@chromium.org>
Auto-Submit: Moe Ahmadi <mahmadi@chromium.org>
Reviewed-by: Justin Donnelly <jdonnelly@chromium.org>
Reviewed-by: dpapad <dpapad@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#930882}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3232178
Cr-Commit-Position: refs/branch-heads/4638@{#922}
Cr-Branched-From: 159257cab5585bc8421abf347984bb32fdfe9eb9-refs/heads/main@{#920003}

[modify] https://crrev.com/7095119c76ff55ed7e1706f6728cd98476e69f98/chrome/browser/resources/new_tab_page/realbox/realbox_match.js

Comment 50 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 51 by ashis...@gmail.com on Wed, Oct 20, 2021, 4:07 PM EDT

To answer #Comment 50:

Hello,

I would like to understand why only 1000 was paid for Universal XSS where I have already showed the impact as this was not only the javascript execution only for one user it was affecting all users as I was able to execute javascript on any user Google Chrome browser and for that I have sent two poc video. Please explain me.

Thank you

Comment 52 by amyressler@chromium.org on Wed, Oct 20, 2021, 4:35 PM EDT Project Member

Hello Ashish, the VRP Panel did fully review the report and POC videos while assessing this report. The impact of this bug does not result in a universal XSS, but XSS solely on the NTP. The impact of exploitation via this XSS bug does not allow for arbitrary JS execution universally across Chrome, thus warranting it a "universal XSS" and allowing for an attacker to extract a victim's gmail cookies, for example.
If you can demonstrate this level of exploitability via this issue, we would welcome that information and would be happy to reassess this issue.
Thank you!

Comment 53 by amyressler@chromium.org on Wed, Oct 20, 2021, 4:37 PM EDT Project Member

Following up to Comment #50, thank you for this report and please let us know the name/handle you would like us to use in acknowledging you for this issue.

Comment 54 by ashis...@gmail.com on Wed, Oct 20, 2021, 4:41 PM EDT

Reply to #Comment 53:

Ashish Arun Dhone

https://in.linkedin.com/in/ashish-dhone-640489135

Comment 55 by amyressler@google.com on Thu, Oct 21, 2021, 4:41 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 56 by tsepez@chromium.org on Mon, Oct 25, 2021, 2:07 PM EDT Project Member

~~Issue 1262830~~ has been merged into this issue.

Comment 57 by rzanoni@google.com on Thu, Oct 28, 2021, 11:18 AM EDT Project Member

Labels: LTS-Security-90 LTS-Security-NotApplicable-90

Not reproducible on M90, innerHTML isn't used in computeMatchText_().

Comment 58 by amyressler@chromium.org on Thu, Oct 28, 2021, 11:39 AM EDT Project Member

Labels: Release-1-M95

Comment 59 by ashis...@gmail.com on Thu, Oct 28, 2021, 11:48 AM EDT

Hello Team,

Any update regarding Bounty? Is it like the same process we get from Google VRP or do I have to fill any form somewhere ?

Thank you

Comment 60 by amyressler@chromium.org on Thu, Oct 28, 2021, 11:53 AM EDT Project Member

Hi, Ashish, the payment process for Chrome VRP is the same as Google VRP, which goes through the same finance team. Please reach out to p2p-vrp@google.com with questions about payment status.

Comment 61 by ashis...@gmail.com on Thu, Oct 28, 2021, 11:54 AM EDT

Thank you very much for the update :)

Comment 62 by amyressler@google.com on Thu, Oct 28, 2021, 12:11 PM EDT Project Member

Labels: CVE-2021-37999 CVE_description-missing

Comment 63 by adetaylor@google.com on Mon, Nov 1, 2021, 3:31 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

Marking this as public earlier than normal, after discussion with tsepez@ and amyressler@, because we keep getting duplicates reported.

Comment 64 by mahmadi@chromium.org on Mon, Nov 1, 2021, 3:55 PM EDT Project Member

~~Issue 1263852~~ has been merged into this issue.

Comment 65 by tsepez@chromium.org on Thu, Nov 4, 2021, 2:58 PM EDT Project Member

~~Issue 1266206~~ has been merged into this issue.

Comment 66 by amyressler@google.com on Tue, Nov 23, 2021, 4:34 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 67 by tsepez@chromium.org on Wed, Jan 5, 2022, 4:41 PM EST Project Member

~~Issue 1284747~~ has been merged into this issue.

Comment 68 by ajgo@google.com on Mon, Jun 27, 2022, 1:40 PM EDT Project Member

Issue 1337578 has been merged into this issue.