☆ Starred by 1 user

Owner:	tluk@chromium.org **Last visit 18 days ago**
CC:	yuhengh@chromium.org adetaylor@google.com
Status:	Fixed *(Closed)*
Components:	----
Modified:	Jun 15, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-02-11
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-Medium
allpublic
CVE_description-submitted
M-89
Target-89
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
Release-0-M89
merge-merged-4389
merge-merged-89
CVE-2021-21180

Issue 1175507: Security: heap-use-after-free in TabSearchPageHandler::CloseTab

Reported by abalq...@microsoft.com on Sat, Feb 6, 2021, 11:28 PM EST

Code

VULNERABILITY DETAILS
When tabsearch closes itself whilst having its webui url loaded UAF crash is observed.

VERSION
Chrome Version: 90.0.4411.0 (Developer Build) (64-bit)
Operating System: Windows 10 Pro

REPRODUCTION CASE
1. Open Chrome and create a new tab/window
2. navigate that window/tab to 'chrome://tab-search.top-chrome/'
3. Within 'chrome://tab-search.top-chrome/' press the 'x' next to the tab corresponding to itself.

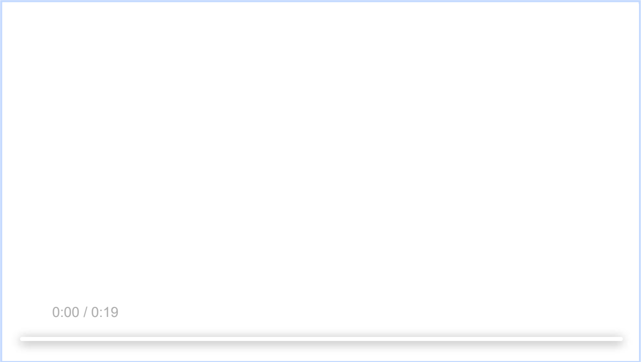
crash occurs, see attached video for live demo.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State: see attached asan log

CREDIT INFORMATION
Reporter credit: Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research

tabsearchasan.txt
20.0 KB View Download

tabsearch.mp4
858 KB View Download



Comment 1 by tsepez@chromium.org on Mon, Feb 8, 2021, 1:03 PM EST Project Member

Owner: tbergquist@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable Pri-1
Components: UI>Browser>TabStrip

Assigning per the other recent tabstrip issues.

Comment 2 by sheriffbot on Mon, Feb 8, 2021, 1:03 PM EST Project Member

Labels: Target-89 M-89

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 tbergquist@chromium.org on Mon, Feb 8, 2021, 1:34 PM EST Project Member

Owner: tluk@chromium.org
Components: -UI>Browser>TabStrip UI>Browser>TabSearch

This looks pretty much like a tab search specific issue. Forwarding to the right people (or closer, at least).

Comment 4 by sheriffbot on Mon, Feb 8, 2021, 2:33 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 5 by tluk@chromium.org on Mon, Feb 8, 2021, 3:13 PM EST Project Member

Labels: OS-Windows

Taking a look

Comment 6 by tluk@chromium.org on Mon, Feb 8, 2021, 7:52 PM EST Project Member

CL up for review, will be requesting a merge through to M88.
https://crrev.com/c/2683300

Comment 7 by tluk@chromium.org on Mon, Feb 8, 2021, 8:02 PM EST Project Member

Cc: yuhengh@chromium.org

Comment 8 by bugdroid on Tue, Feb 9, 2021, 10:55 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/8bce82107db385608344d9656c69ff8cd467229b

commit 8bce82107db385608344d9656c69ff8cd467229b
Author: Tom <tluk@chromium.org>
Date: Tue Feb 09 15:54:46 2021

Tab Search: Fix CloseTab() sequencing error in TabSearchPageHandler

This CL addresses a UAF memory error that occurs when closing the Tab
Search WebUI from within a browser tab.

When CloseTab() is called it calls CloseWebContentsAt() which
synchronously closes and destroys the target WebContents. When
CloseTab() is called on the browser tab WebContents hosting Tab
Search, this results in destruction of the TabSearchUI and its
TabSearchPageHandler.

This CL ensures that the TabSearchPageHandler does not perform
any additional actions following the call to CloseWebContentsAt().

~~Bug: 1175507~~
Change-Id: Ie7af8345eb6f8dc9352e733958b4ec01155da740
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2683300
Commit-Queue: Thomas Lukaszewicz <tluk@chromium.org>
Reviewed-by: Yuheng Huang <yuhengh@chromium.org>
Cr-Commit-Position: refs/heads/master@{#852208}

[modify] https://crrev.com/8bce82107db385608344d9656c69ff8cd467229b/chrome/browser/ui/webui/tab_search/tab_search_page_handler_unittest.cc
[modify] https://crrev.com/8bce82107db385608344d9656c69ff8cd467229b/chrome/browser/ui/webui/tab_search/tab_search_page_handler.cc
[modify] https://crrev.com/8bce82107db385608344d9656c69ff8cd467229b/chrome/browser/ui/webui/tab_search/tab_search_ui_browsertest.cc

Comment 9 by tluk@chromium.org on Tue, Feb 9, 2021, 11:32 AM EST Project Member

Labels: Merge-Request-89

Requesting merge to branch M89.

Comment 10 by pbommana@google.com on Tue, Feb 9, 2021, 3:02 PM EST Project Member

tluk@ setting the next action date to 02/11/2021, Since Change landed but not made it to canary yet, so let's wait for canary coverage and verification please. thank you.

Comment 11 by pbommana@google.com on Tue, Feb 9, 2021, 3:02 PM EST Project Member

NextAction: 2021-02-11

Comment 12 by adetaylor@chromium.org on Tue, Feb 9, 2021, 5:00 PM EST Project Member

Please mark this as Fixed if it is. (https://chromium.googlesource.com/chromium/src/+/master/docs/security/security-labels.md#toc-merge-labels)

Comment 13 by tluk@chromium.org on Tue, Feb 9, 2021, 5:02 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 14 by sheriffbot on Wed, Feb 10, 2021, 10:59 AM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89's targeted beta branch promotion date has already passed, so this requires manual review
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: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 15 by sheriffbot on Wed, Feb 10, 2021, 1:57 PM EST Project Member

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

Comment 16 by adetaylor@google.com on Fri, Feb 12, 2021, 1:34 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389, assuming no problems have shown up in Canary.

Comment 17 by sheriffbot on Tue, Feb 16, 2021, 12:13 PM EST Project Member

Cc: adetaylor@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 18 by bugdroid on Tue, Feb 16, 2021, 6:12 PM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/30c51a7da4763ac893536dbfec6e2c121c36c041

commit 30c51a7da4763ac893536dbfec6e2c121c36c041
Author: tom <tluk@chromium.org>
Date: Tue Feb 16 23:05:26 2021

[M89 Merge] Tab Search: Fix CloseTab() sequencing error in TabSearchPageHandler

This CL addresses a UAF memory error that occurs when closing the Tab Search WebUI from within a browser tab.

When CloseTab() is called it calls CloseWebContentsAt() which synchronously closes and destroys the target WebContents. When CloseTab() is called on the browser tab WebContents hosting Tab Search, this results in destruction of the TabSearchUI and its TabSearchPageHandler.

This CL ensures that the TabSearchPageHandler does not perform any additional actions following the call to CloseWebContentsAt().

(cherry picked from commit 8bce82107db385608344d9656c69ff8cd467229b)

~~Bug: 1175507~~
Change-Id: Ie7af8345eb6f8dc9352e733958b4ec01155da740
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2683300
Commit-Queue: Thomas Lukaszewicz <tluk@chromium.org>
Reviewed-by: Yuheng Huang <yuhengh@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#852208}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2698233
Cr-Commit-Position: refs/branch-heads/4389@{#1117}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/30c51a7da4763ac893536dbfec6e2c121c36c041/chrome/browser/ui/webui/tab_search/tab_search_page_handler_unittest.cc
[modify] https://crrev.com/30c51a7da4763ac893536dbfec6e2c121c36c041/chrome/browser/ui/webui/tab_search/tab_search_page_handler.cc
[modify] https://crrev.com/30c51a7da4763ac893536dbfec6e2c121c36c041/chrome/browser/ui/webui/tab_search/tab_search_ui_browsertest.cc

Comment 19 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 20 by adetaylor@google.com on Mon, Mar 1, 2021, 7:28 PM EST Project Member

Labels: CVE-2021-21180 CVE_description-missing

Comment 21 by vsavu@google.com on Wed, Mar 3, 2021, 5:04 AM EST Project Member

Labels: LTS-Merge-Request-86

Comment 22 by vsavu@google.com on Wed, Mar 3, 2021, 5:59 AM EST Project Member

Labels: LTS-Security-86

Comment 23 by gianluca@google.com on Wed, Mar 3, 2021, 10:33 AM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 24 by Git Watcher on Tue, Mar 9, 2021, 9:36 AM EST Project Member

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/729c6bc6b10c7773d7081e6bd9a63435a9c679e4

commit 729c6bc6b10c7773d7081e6bd9a63435a9c679e4
Author: tom <tluk@chromium.org>
Date: Tue Mar 09 14:35:42 2021

[M86-LTS] Tab Search: Fix CloseTab() sequencing error in TabSearchPageHandler

This CL addresses a UAF memory error that occurs when closing the Tab
Search WebUI from within a browser tab.

When CloseTab() is called it calls CloseWebContentsAt() which
synchronously closes and destroys the target WebContents. When
CloseTab() is called on the browser tab WebContents hosting Tab
Search, this results in destruction of the TabSearchUI and its
TabSearchPageHandler.

This CL ensures that the TabSearchPageHandler does not perform
any additional actions following the call to CloseWebContentsAt().

[M86 Merge]: Dropped test changes due to conflicts.

(cherry picked from commit 8bce82107db385608344d9656c69ff8cd467229b)

(cherry picked from commit 30c51a7da4763ac893536dbfec6e2c121c36c041)

~~Bug: 1175507~~
Change-Id: Ie7af8345eb6f8dc9352e733958b4ec01155da740
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2683300
Commit-Queue: Thomas Lukaszewicz <tluk@chromium.org>
Reviewed-by: Yuheng Huang <yuhengh@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#852208}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2698233
Cr-Original-Commit-Position: refs/branch-heads/4389@{#1117}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2731807
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1568}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/729c6bc6b10c7773d7081e6bd9a63435a9c679e4/chrome/browser/ui/webui/tab_search/tab_search_page_handler.cc
[modify] https://crrev.com/729c6bc6b10c7773d7081e6bd9a63435a9c679e4/chrome/browser/ui/webui/tab_search/tab_search_page_handler_unittest.cc

Comment 25 by vsavu@google.com on Tue, Mar 9, 2021, 11:03 AM EST Project Member

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

Comment 26 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 27 by sheriffbot on Tue, Jun 15, 2021, 1:52 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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