☆ Starred by 2 users

Owner:	yuezhanggg@chromium.org
CC:	wychen@chromium.org ayman@chromium.org meili...@chromium.org yuezhanggg@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Shopping>Cart
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Mac
Pri:	1
Type:	Bug-Security

Needs-Feedback
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
reward-16000
external_security_report
M-98
Target-98
FoundIn-97
Security_Impact-Extended
Release-0-M100
CVE-2022-1135

Issue 1285601: Security: heap-use-after-use in DiscountURLLoader::NavigateToDiscountURL

Reported by yuanv...@gmail.com on Sat, Jan 8, 2022, 11:11 AM EST

Code

VULNERABILITY DETAILS

If we login a user and visit a url match cart rules, CartService will be created for the profile. When CartService construct, |cart_db_| initializing and so is the ProfileProtoDB instance |cart_db_->proto_db_|. The initialization of ProfileProtoDB is an async task run on background thread and will post ProfileProtoDB::OnDatabaseInitialized task to UI thread when it finished. Before ProfileProtoDB initialized, all queries to it will be stored in |deferred_operations_| and deferred running in OnDatabaseInitialized.

DiscountURLLoader::TabChangedAt has a callchain like |CartService::GetDiscountURL => CartService::LoadCart => CartDB::LoadCart => ProfileProtoDB<T>::LoadOneEntry|, if this happened before |cart_db_| initialized, callback binds with raw WebContents pointer will be stored. The WebContents could be destoryed before the callback run, UaF triggered in DiscountURLLoader::NavigateToDiscountURL.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/persisted_state_db/profile_proto_db.h;drc=ce55a875516951f56c738b4527eb17ec9de7b6b1;l=383
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/persisted_state_db/profile_proto_db.h;drc=ce55a875516951f56c738b4527eb17ec9de7b6b1;l=393

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/cart/discount_url_loader.cc;l=41

```
void DiscountURLLoader::TabChangedAt(content::WebContents* contents,
                                     int index,
                                     TabChangeType change_type) {
  ...
    if (last_interacted_url_ == contents->GetVisibleURL()) {
      cart_service_->GetDiscountURL(
          contents->GetVisibleURL(),
          base::BindOnce(&DiscountURLLoader::NavigateToDiscountURL,
                         weak_ptr_factory_.GetWeakPtr(), contents));          // callback bind with raw WebContents ptr
    }
   ...
}
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/persisted_state_db/profile_proto_db.h;drc=ce55a875516951f56c738b4527eb17ec9de7b6b1;l=180

```
void ProfileProtoDB<T>::LoadOneEntry(const std::string& key,
                                     LoadCallback callback) {
  if (InitStatusUnknown()) {                         // if db is still initializing, callback be stored in |deferred_operations_|
    deferred_operations_.push_back(base::BindOnce(
        &ProfileProtoDB::LoadOneEntry, weak_ptr_factory_.GetWeakPtr(), key,
        std::move(callback)));
  } else if (FailedToInit()) {
  ...
}
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/cart/discount_url_loader.cc;l=57

```
void DiscountURLLoader::NavigateToDiscountURL(content::WebContents* contents,
                                              const GURL& discount_url) {
```

```
                                              const GURL& discount_url) {
  contents->GetController().LoadURL(discount_url, content::Referrer(),      // raw WebContents ptr use here may trigger UaF
                                    ui::PAGE_TRANSITION_FIRST, std::string());
}
```

Fix suggestions:
1. use weakptr or observe the webcontents
2. dynamic get webcontents in callback again

VERSION
Chrome Version: stable (according to source code)
Operating System: except Android (CartServcie not work on android)

REPRODUCTION CASE
I am not familiar with cart module and still investigating it. The steps below is analysed from source code.

1. Enable cart and discount features in chrome and login a user. (I am still confused about these cart and discount rules)
2. Prepare a large profile database or try slowly IO. (lengthen cart database initialize time)
3. Visit a ruled url like 'https://www.nike.com/cart' (contruct CartService)
4. Trigger CartService::PrepareForNavigation through action or Mojo call (construct DiscountURLLoader instance in CartService and set |last_interacted_url_|)
5. Refresh tab (trigger DiscountURLLoader::TabChangedAt with TabChangeType::kAll) and close it. (destory the WebContents,)
6. UaF may trigger soon. (cart database initialized and run callbacks)

Even there are lots of limits to trigger the bug, the race condition problem may could be triggerred by Mojo and lead to sandbox escape.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser

CREDIT INFORMATION
Reporter credit: Wei Yuan(@vo_sec) of MoyunSec VLab

Comment 1 by sheriffbot on Sat, Jan 8, 2022, 11:13 AM EST   Project Member

Labels: external_security_report

Comment 2 by drubery@chromium.org on Mon, Jan 10, 2022, 4:37 PM EST   Project Member

Cc: wychen@chromium.org
Labels: Needs-Feedback
Components: UI>Browser>Shopping>Cart

It would be great if you could get some kind of reliable reproduction steps, but for now CC'ing a code owner to see whether they think this is plausible.

Comment 3 by ajgo@google.com on Tue, Jan 18, 2022, 2:58 PM EST   Project Member

Owner: wychen@chromium.org
Cc: ayman@chromium.org
Labels: Security_Severity-Medium FoundIn-97

wychen: ptal - it would be good to know if these features currently enabled (in M97 or later?) - if you are not the right person to investigate please assign to someone else - thanks.

Comment 4 by sheriffbot on Tue, Jan 18, 2022, 2:59 PM EST Project Member

Labels: Security_Impact-Stable

Comment 5 by yuezhanggg@chromium.org on Tue, Jan 18, 2022, 3:57 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: yuezhanggg@chromium.org
Labels: OS-Linux OS-Mac OS-Windows Pri-2

Thanks for filing! This is a great catch. I can take this one as I wrote that part of code.

Comment 6 by sheriffbot on Wed, Jan 19, 2022, 12:51 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of medium severity.

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

Comment 7 by sheriffbot on Wed, Jan 19, 2022, 1:17 PM EST 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 8 by Git Watcher on Tue, Feb 1, 2022, 1:06 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5b399d63e31334d6d61125f039907a0c5d358a50

commit 5b399d63e31334d6d61125f039907a0c5d358a50
Author: Yue Zhang <yuezhanggg@chromium.org>
Date: Tue Feb 01 18:05:45 2022

[RBD] Fix potential use-after-destroy of WebContents

~~Bug: 1285601~~
Change-Id: I7ed33e13189a024946bfad9ef9ec58f2d777b60f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3402408
Reviewed-by: Wei-Yin Chen <wychen@chromium.org>
Commit-Queue: Yue Zhang <yuezhanggg@chromium.org>
Cr-Commit-Position: refs/heads/main@{#965763}

[modify] https://crrev.com/5b399d63e31334d6d61125f039907a0c5d358a50/chrome/browser/cart/discount_url_loader.cc
[modify] https://crrev.com/5b399d63e31334d6d61125f039907a0c5d358a50/chrome/browser/cart/discount_url_loader.h

Comment 9 by sheriffbot on Tue, Feb 1, 2022, 5:37 PM EST Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 10 by sheriffbot on Wed, Feb 2, 2022, 12:21 PM EST Project Member

yuezhanggg: 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 11 by yuezhanggg@chromium.org on Wed, Feb 2, 2022, 12:23 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 12 by sheriffbot on Wed, Feb 2, 2022, 12:45 PM EST Project Member

Labels: reward-topanel

Comment 13 by sheriffbot on Wed, Feb 2, 2022, 1:45 PM EST Project Member

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

Comment 14 by amyressler@google.com on Wed, Feb 23, 2022, 3:05 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-16000

*** 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 15 by amyressler@chromium.org on Wed, Feb 23, 2022, 3:10 PM EST Project Member

Congratulations -- the VRP Panel has decided to award you $16,000 for this report. Thank you for your efforts and nice work!

Comment 16 by amyressler@google.com on Fri, Feb 25, 2022, 8:53 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 17 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:13 PM EDT Project Member

Labels: Release-0-M100

Comment 18 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

Labels: CVE-2022-1135 CVE_description-missing

Comment 19 by sheriffbot on Wed, May 11, 2022, 1:31 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

Comment 20 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 21 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy