Starred by 4 users

| | |
|---|---|
| **Owner:** | xinghuilu@chromium.org |
| **CC:** | drubery@chromium.org<br>vakh@chromium.org |
| **Status:** | Fixed *(Closed)* |
| **Components:** | Services>Safebrowsing |
| **Modified:** | Jul 21, 2022 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Android |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
SafeBrowsing-Triaged
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-81
reward-16000
external_security_report
M-98
Target-98
Security_Impact-Extended
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0979

## Issue 1302644: Security: Use After Free in ChromePasswordProtectionService::HandleUserActionOnModalWarning

Reported by karth...@gmail.com on Thu, Mar 3, 2022, 9:31 AM EST

Code

**VULNERABILITY DETAILS**

Root cause: The class PasswordReuseControllerAndroid derived from WebContentsObserver but does not observe any WebContents which will lead to UAF.

Class link:
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/safe_browsing/android/password_reuse_controller_android.h;drc=57665886a1bb4533871c9b28f1e6b977755457e3;l=31

Class definition:

```
class PasswordReuseControllerAndroid
    : public ChromePasswordProtectionService::Observer,
      public content::WebContentsObserver
```

Class constructor implementation:

```
PasswordReuseControllerAndroid::PasswordReuseControllerAndroid(
    content::WebContents* web_contents,
    ChromePasswordProtectionService* service,
    ReusedPasswordAccountType password_type,
    OnWarningDone done_callback)
    : service_(service),
      url_(web_contents->GetLastCommittedURL()),
      password_type_(password_type),
      window_android_(web_contents->GetTopLevelNativeWindow()),
      done_callback_(std::move(done_callback))
```

Detail: Chrome will show a warning dialog when user input a password on a website marked as phishing (etc.) and the input was detected reusing existing passwords stored.

Based on the code below, on Android devices, it will create a new instance of PasswordReuseControllerAndroid. Because PasswordReuseControllerAndroid does not observe web_contents, PasswordReuseControllerAndroid won't be notified when the web_contents was destroyed.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/safe_browsing/chrome_password_protection_service.cc;l=428;drc=57665886a1bb4533871c9b28f1e6b977755457e3

```
(new PasswordReuseControllerAndroid(
      web_contents, this, password_type,
      base::BindOnce(&ChromePasswordProtectionService::OnUserAction,
                     base::Unretained(this), web_contents, password_type,
                     outcome, verdict_type, verdict_token,
                     WarningUIType::MODAL_DIALOG)))

     ->ShowDialog();
```

When the user clicks any button on the dialog, it will call OnUserAction. Since the parameter bound on the OnUserAction function is a raw point points to web_contents, it will cause UAF when the raw pointer is accessed in HandleUserActionOnModalWarning.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/safe_browsing/chrome_password_protection_service.cc;l=947;drc=57665886a1bb4533871c9b28f1e6b977755457e3

```
void ChromePasswordProtectionService::HandleUserActionOnModalWarning(
    content::WebContents* web_contents,
    ReusedPasswordAccountType password_type,
    RequestOutcome outcome,
    LoginReputationClientResponse::VerdictType verdict_type,
    const std::string& verdict_token,
    WarningAction action) {
  const Origin origin = web_contents->GetMainFrame()->GetLastCommittedOrigin();
```

**VERSION**
Chrome Version: [99.0.4844.48] + [stable]
Operating System: [Android]

**REPRODUCTION CASE**

1. Apply the patch and compile Chromium. This patch was meant to simulate a response from google service to mark the website as phishing.

NOTE: Please disconnect the network before the next step to avoid interference caused by the google server response.

2. Setup httpserver

adb reverse tcp:8000 tcp:8000
python -m SimpleHTTPServer 8000

3. Run
out/Android_Asan/bin/chrome_public_apk launch --args="--host-rules=\"MAP phishing.com 127.0.0.1\""

4. Navigate to http://localhost:8000/poc.html

5. Click 'Save' on Save Password prompt

All the steps above are meant to simulate a customer save a password on the device.

6. Click 'Click Me' button, type in '11111111', wait for the warning dialog to show up. Then wait for the page to be closed (Note: The warning should show up before the page was closed).

7. Click any button on the dialog

FIX
The attached fix.diff shows my suggestion about how to fix this issue.

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

**CREDIT INFORMATION**
**Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?**
Reporter credit: anonymous

**patch.diff**
1.5 KB View Download

**child.html**
302 bytes View Download

**poc.html**
1.2 KB View Download

**asan.log**
16.4 KB View Download

**fix.diff**
830 bytes View Download

Comment 1 by sheriffbot on Thu, Mar 3, 2022, 9:31 AM EST

**Labels:** external_security_report

Comment 2 Deleted

Comment 3 by dcheng@chromium.org on Thu, Mar 3, 2022, 3:19 PM EST

**Status:** Assigned (was: Unconfirmed)
**Owner:** xinghuilu@chromium.org
**Labels:** FoundIn-81 Security_Severity-Critical Security_Severity-High OS-Android Pri-1
**Components:** Services>Safebrowsing

Good find!

Normally, a browser process UaF would be critical. I'm going to tentatively mark this as high due to the user interaction required.

Comment 4 by sheriffbot on Thu, Mar 3, 2022, 3:20 PM EST

**Labels:** Security_Impact-Extended

Comment 5 by sheriffbot on Fri, Mar 4, 2022, 12:47 PM EST

**Labels:** M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 6 by sheriffbot on Fri, Mar 4, 2022, 1:13 PM EST

**Labels:** -Pri-1 Pri-0

Setting Pri-0 to match security severity Critical. 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 7 by xinghuilu@chromium.org on Fri, Mar 4, 2022, 2:00 PM EST

**Status:** Started (was: Assigned)
**Cc:** drubery@chromium.org
**Labels:** -Security_Severity-Critical

Thanks for the detailed report! I'm able to reproduce and the issue is indeed a miss of observing the WebContents.

Agree that the severity is high because of the additional user interaction. And that triggering the modal requires the Google server to return phishing or low_reputation verdict, which is rare.

Comment 8 by xinghuilu@chromium.org on Fri, Mar 4, 2022, 6:46 PM EST

**Labels:** SafeBrowsing-Triaged

Comment 9 by Git Watcher on Tue, Mar 8, 2022, 1:34 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1e71a1fcad627e61585d023aa2102262c1dc35b7

commit 1e71a1fcad627e61585d023aa2102262c1dc35b7
Author: Xinghui Lu <xinghuilu@chromium.org>
Date: Tue Mar 08 06:33:37 2022

Destroy PasswordReuseControllerAndroid on web contents destruction.

Previously the WebContentsObserver is not properly bound in the
controller's constructor.

~~Bug: 1302644~~
Change-Id: Ic22976d4c2e1fff0bacda024415b71c1536d9606
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503938
Reviewed-by: Daniel Rubery <drubery@chromium.org>
Commit-Queue: Xinghui Lu <xinghuilu@chromium.org>
Cr-Commit-Position: refs/heads/main@{#978619}

[modify]
https://crrev.com/1e71a1fcad627e61585d023aa2102262c1dc35b7/chrome/browser/safe_browsing/android/password_reuse_controller_android_unittest.cc
[modify]

https://crrev.com/1e71a1fcad627e61585d023aa2102262c1dc35b7/chrome/browser/safe_browsing/android/password_reuse_controller_android.cc

Comment 10 by xinghuilu@chromium.org on Tue, Mar 8, 2022, 2:01 PM EST

**Status:** Fixed (was: Started)

Comment 11 by sheriffbot on Tue, Mar 8, 2022, 2:02 PM EST

**Labels:** Merge-Request-100 Merge-Request-98 Merge-Request-99

Requesting merge to extended stable M98 because latest trunk commit (978619) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (978619) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (978619) appears to be after beta branch point (972766).

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

Comment 12 by amyressler@chromium.org on Tue, Mar 8, 2022, 6:14 PM EST

**Labels:** Pri-1

adjusting pri to reflect severity; thanks for the quick fix, Xinghui.
Since this landed, I'm going this get a bit more bake time on Canary. Let's revisit tomorrow to see if this makes senes to merge by Thursday so this can be in the next security respin for 99/Stable, given that it's rather small and seems pretty low risk.

Comment 13 by sheriffbot on Wed, Mar 9, 2022, 1:34 AM EST

**Labels:** -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 is already shipping to beta.

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), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 14 by sheriffbot on Wed, Mar 9, 2022, 1:34 AM EST

**Labels:** -Merge-Request-99 Merge-Review-99

Merge review required: M99 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 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), ceb (ChromeOS), pbommana (Desktop)

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

Comment 15 by sheriffbot on Wed, Mar 9, 2022, 1:34 AM EST

**Labels:** -Merge-Request-98 Merge-Review-98

Merge review required: M98 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 16 by sheriffbot on Wed, Mar 9, 2022, 12:42 PM EST

**Labels:** reward-topanel

Comment 17 by xinghuilu@chromium.org on Wed, Mar 9, 2022, 1:22 PM EST

1. Yes. High severity security bug.
2. https://crrev.com/c/3503938
3. Yes.
4. No.
5. N/A
6. No, not a new feature.

Comment 18 by sheriffbot on Wed, Mar 9, 2022, 1:42 PM EST

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

Comment 19 by amyressler@chromium.org on Wed, Mar 9, 2022, 5:37 PM EST

**Labels:** -Merge-Review-98 -Merge-Review-99 -Merge-Review-100 Merge-Approved-100 Merge-Approved-99 Merge-

Approved-98

M100 merge approved, please merge to branch 4896

M99 merge approved, please merge this fix to branch 4844 by noon PST tomorrow/Thursday, 10 March so this fix can be included in the next stable security refresh

M98 merge approved, please merge to branch 4758 so this fix can be included in Extended Stable respin -- thank you!

Comment 20 by Git Watcher on Wed, Mar 9, 2022, 8:00 PM EST

**Labels:** -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/eb9f2c2099e901d4faacdbc9ce72fb5d5edbf8fc

commit eb9f2c2099e901d4faacdbc9ce72fb5d5edbf8fc
Author: Xinghui Lu <xinghuilu@chromium.org>
Date: Thu Mar 10 00:59:17 2022

[M100] Destroy PasswordReuseControllerAndroid on web contents destruction.

Previously the WebContentsObserver is not properly bound in the
controller's constructor.

(cherry picked from commit 1e71a1fcad627e61585d023aa2102262c1dc35b7)

~~Bug: 1302644~~
Change-Id: Ic22976d4c2e1fff0bacda024415b71c1536d9606
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503938
Reviewed-by: Daniel Rubery <drubery@chromium.org>
Commit-Queue: Xinghui Lu <xinghuilu@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#978619}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3514818
Auto-Submit: Xinghui Lu <xinghuilu@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4896@{#432}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/eb9f2c2099e901d4faacdbc9ce72fb5d5edbf8fc/chrome/browser/safe_browsing/android/password_reuse_controller_android_unittest.cc
[modify]
https://crrev.com/eb9f2c2099e901d4faacdbc9ce72fb5d5edbf8fc/chrome/browser/safe_browsing/android/password_reuse_controller_android.cc

Comment 21 by Git Watcher on Wed, Mar 9, 2022, 8:54 PM EST

**Labels:** -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6e896d17286cb976555b0b672d32ffea2ab95562

commit 6e896d17286cb976555b0b672d32ffea2ab95562
Author: Xinghui Lu <xinghuilu@chromium.org>
Date: Thu Mar 10 01:53:46 2022

Date: Thu Mar 10 01:53:46 2022

[M99] Destroy PasswordReuseControllerAndroid on web contents destruction.

Previously the WebContentsObserver is not properly bound in the
controller's constructor.

(cherry picked from commit 1e71a1fcad627e61585d023aa2102262c1dc35b7)

~~Bug: 1302644~~
Change-Id: Ic22976d4c2e1fff0bacda024415b71c1536d9606
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503938
Reviewed-by: Daniel Rubery <drubery@chromium.org>
Commit-Queue: Xinghui Lu <xinghuilu@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#978619}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3514286
Auto-Submit: Xinghui Lu <xinghuilu@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4844@{#1026}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]
https://crrev.com/6e896d17286cb976555b0b672d32ffea2ab95562/chrome/browser/safe_browsing/android/password_reuse_controller_android_unittest.cc
[modify]
https://crrev.com/6e896d17286cb976555b0b672d32ffea2ab95562/chrome/browser/safe_browsing/android/password_reuse_controller_android.cc

Comment 22 by Git Watcher on Wed, Mar 9, 2022, 8:58 PM EST

**Labels:** -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b756e611c62ef992a27d20a148dbcf63c7c7e6fa

commit b756e611c62ef992a27d20a148dbcf63c7c7e6fa
Author: Xinghui Lu <xinghuilu@chromium.org>
Date: Thu Mar 10 01:57:18 2022

[M98] Destroy PasswordReuseControllerAndroid on web contents destruction.

Previously the WebContentsObserver is not properly bound in the
controller's constructor.

(cherry picked from commit 1e71a1fcad627e61585d023aa2102262c1dc35b7)

~~Bug: 1302644~~
Change-Id: Ic22976d4c2e1fff0bacda024415b71c1536d9606
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503938
Reviewed-by: Daniel Rubery <drubery@chromium.org>
Commit-Queue: Xinghui Lu <xinghuilu@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#978619}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3514935
Auto-Submit: Xinghui Lu <xinghuilu@chromium.org>

Auto-Submit: Xinghui Lu <xinghuilu@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4758@{#1242}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify]
https://crrev.com/b756e611c62ef992a27d20a148dbcf63c7c7e6fa/chrome/browser/safe_browsing/android/password_reuse_controller_android_unittest.cc
[modify]
https://crrev.com/b756e611c62ef992a27d20a148dbcf63c7c7e6fa/chrome/browser/safe_browsing/android/password_reuse_controller_android.cc

Comment 23 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:23 PM EST

**Labels:** Release-1-M99

Comment 24 by amyressler@google.com on Mon, Mar 14, 2022, 6:14 PM EDT

**Labels:** CVE-2022-0979 CVE_description-missing

Comment 25 by amyressler@google.com on Wed, Mar 16, 2022, 9:46 PM EDT

**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 26 by amyressler@chromium.org on Wed, Mar 16, 2022, 10:23 PM EDT

Congratulations! The VRP Panel has decided to award you $15,000 for this report and a $1,000 patch bonus. Thank you for your efforts and excellent work!

Comment 27 by amyressler@google.com on Thu, Mar 17, 2022, 5:22 PM EDT

**Labels:** -reward-unpaid reward-inprocess

Comment 28 by sheriffbot on Wed, Jun 15, 2022, 1:31 PM EDT

**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 29 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT

**Labels:** CVE_description-submitted -CVE_description-missing

Comment 30 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:19 PM EDT

**Labels:** -CVE_description-missing --CVE_description-missing