Starred by 2 users

Owner:	dpa...@chromium.org
CC:	yelizaveta@google.com maybelle@chromium.org dpa...@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Settings
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Needs-Feedback
Security_Impact-Stable
Security_Severity-Medium
reward-7500
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
Release-0-M101
CVE-2022-1484

Issue 1297429: [WebUI] StartupPagesHandler does not adequately verify arguments from JS

Reported by happy...@gmail.com on Tue, Feb 15, 2022, 12:15 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.1 Safari/605.1.15

Steps to reproduce the problem:
1.

What is the expected behavior?

What went wrong?
Will comment it soon.

Did this work before? N/A

Chrome version: Channel: n/a
OS Version:

Comment 1 by sheriffbot on Tue, Feb 15, 2022, 12:17 AM EST

Labels: external_security_report

Comment 2 by happy...@gmail.com on Tue, Feb 15, 2022, 12:21 AM EST

In [1], HandleAddStartupPage function doesn't verify if the `args[1]` is a String type variant, and get it as String directly.

In [2], index from `args[1].GetInt()` doesn't check whether it is less than 0. If the index is less than 0, heap overflow will happened in [3].

Note that index could be controlled by sending UI message in JS, when there's a uxss in chromium.

[1].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/settings_startup_pages_handler.cc;l=112;drc=2d5863b4bd4a723b2cbaa4cc708f1ebf7682f9ff

[2].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/settings_startup_pages_handler.cc;l=122-123;drc=2d5863b4bd4a723b2cbaa4cc708f1ebf7682f9ff

[3].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/settings_startup_pages_handler.cc;l=125;drc=2d5863b4bd4a723b2cbaa4cc708f1ebf7682f9ff

Comment 3 Deleted

Comment 4 by yelizaveta@google.com on Tue, Feb 15, 2022, 11:34 AM EST

Labels: Needs-Feedback

Hello, in your first example, index is assigned based on the result of calling RowCount[1] which returns the size of a vector, which cannot be less than 0.

For your other examples, do you have a PoC or more evidence that these are vulnerabilities?

Comment 5 by happy...@gmail.com on Tue, Feb 15, 2022, 11:47 AM EST

Thanks for the reply.

Index could be assign by the args[1] which interpreted the value as int in (1). Note that args could be controlled in malicious JS like

chrome,send("addStartupPage", ["test", "test"])

In chrome settings -> startup page.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/settings_startup_pages_handler.cc;drc=2d5863b4bd4a723b2cbaa4cc708f1ebf7682f9ff;l=123

```
if (args[1].is_int() && args[1].GetInt() <= row_count)
  index = args[1].GetInt(); // (1)
```

I currently don't have the PoC for other examples. I think other examples except this index overflow, will only trigger a check assert failure and doesn't have potential security impact.

Comment 6 by happy...@gmail.com on Tue, Feb 15, 2022, 11:51 AM EST

Hence the index could be less than 0 when args[1]<0
Feel free to let me known if I was incorrect.

I recognize it by code inspection, hence the PoC is not available currently. The index pattern is similar as ~~bug 1242392~~.
Thank you.

Comment 7 by sheriffbot on Tue, Feb 15, 2022, 11:51 AM EST

Cc: yelizaveta@google.com
Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 8 by yelizaveta@google.com on Tue, Feb 15, 2022, 12:39 PM EST

Labels: Needs-Feedback

Ah yes I see that now.

It looks like you have the start of a PoC with the malicious JS example you gave. Can you work through that and provide a PoC for controlling args?

Comment 9 by dcheng@chromium.org on Tue, Mar 1, 2022, 7:24 PM EST

Summary: [WebUI] StartupPagesHandler does not adequately verify arguments from JS (was: Inappropriate implementation in StartupPagesHandler)

Status: Assigned (was: Unconfirmed)
Owner: dpa...@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable
Components: UI>Settings

Assigning medium severity since:
1. This is a bug in the validation logic in a browser-side component
2. WebUI is normally isolated into its own renderer process and not typically "malicious"
3. But combined with a UXSS bug that allows arbitrary script execution in a chrome:// renderer would lead to trouble.

Any browser-side code that consumes values from the renderer must validate the values. The missing non-negative index check is possibly the worst example, but a fix for this should also audit the other WebUI message callbacks for other memory safety issues / CHECK issues. A malicious renderer should not be able to trigger either issue, even if it's in a WebUI handler.

Comment 10 by sheriffbot on Wed, Mar 2, 2022, 12:21 PM EST

dpapad: Uh oh! This issue still open and hasn't been updated in the last 15 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 sheriffbot on Wed, Mar 2, 2022, 1:18 PM EST

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 12 Deleted

Comment 13 by happy...@gmail.com on Thu, Mar 3, 2022, 1:49 AM EST

asan.txt
9.5 KB View Download

Comment 14 Deleted

Comment 15 by happy...@gmail.com on Thu, Mar 3, 2022, 4:23 AM EST

Another unchecked index is in [1], | avatar_index | is only guarded by DCHECK, which is not sufficient. However, even if this |avatar_index| could be controlled by any value, it will only trigger CHECK failure [3] in the later access (from my point of code audit.)

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/signin/profile_picker_handler.cc;drc=

fa1dd1718cd4860ad3b9cc4d892812f911bb837f;l=668

```
  size_t avatar_index = args->GetListDeprecated()[2].GetInt(); // [1]
  bool create_shortcut = args->GetListDeprecated()[3].GetBool();
  base::TrimWhitespace(profile_name, base::TRIM_ALL, &profile_name);
  CHECK(!profile_name.empty());

#ifndef NDEBUG
  DCHECK(profiles::IsDefaultAvatarIconIndex(avatar_index)); // [2]
#endif
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/profiles/profile_avatar_icon_util.cc;drc=fa1dd1718cd4860ad3b9cc4d892812f911bb837f;l=495

```
const IconResourceInfo* GetDefaultAvatarIconResourceInfo(size_t index) {
  CHECK_LT(index, kDefaultAvatarIconsCount); // [3]
```

Comment 16 by dpa...@chromium.org on Thu, Mar 3, 2022, 8:32 AM EST

> In [1], HandleAddStartupPage function doesn't verify if the `args[1]` is a String type variant, and get it as String directly.

> In [2], index from `args[1].GetInt()` doesn't check whether it is less than 0. If the index is less than 0, heap overflow will happened in [3].

Candidate fix for HandleAddStartupPage at https://chromium-review.googlesource.com/c/chromium/src/+/3500785.

Comment 17 by Git Watcher on Fri, Mar 4, 2022, 1:10 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/83c1fe8483abf01ca9966c643736048d3f8c2790

commit 83c1fe8483abf01ca9966c643736048d3f8c2790
Author: dpapad <dpapad@chromium.org>
Date: Fri Mar 04 18:09:44 2022

Settings: Remove incorrect logic from HandleAddStartupPage.

The code was trying to parse an index argument from the parameters
passed from JS, but such a parameter is never actually passed from the
UI. Moreover the code that was handling it was incrorectly not checking
for "greater than zero" opening up the door unnecessarily to potential
vulnerabilities, if someose manually passes parameters using the
DevTools console (or if somehow the WebUI page is compromised).

Also changing DCHECK_GE to CHECK_EQ in HandleRemoveStartupPage.

~~Bug: 1297429~~
Change-Id: I1f26c75c5193813c5b5c62e803520706c38c7791
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3500785
Auto-Submit: Demetrios Papadopoulos <dpapad@chromium.org>
Reviewed-by: John Lee <johntlee@chromium.org>

Commit-Queue: John Lee <johntlee@chromium.org>
Cr-Commit-Position: refs/heads/main@{#977725}

[modify]
https://crrev.com/83c1fe8483abf01ca9966c643736048d3f8c2790/chrome/browser/ui/webui/settings/settings_startup_pages_handler.cc

Comment 18 by dpa...@chromium.org on Mon, Mar 7, 2022, 3:11 PM EST

Status: Fixed (was: Assigned)

> I've audit most of the WebUI handlers, and many of them lack the robust check to the size of the arguments.

Can you please file as a separate bug?

Closing this one, as the issues originally identified should now be fixed.

Comment 19 by sheriffbot on Tue, Mar 8, 2022, 12:42 PM EST

Labels: reward-topanel

Comment 20 by sheriffbot on Tue, Mar 8, 2022, 1:41 PM EST

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

Comment 21 by amyressler@google.com on Wed, Mar 16, 2022, 9:46 PM EDT

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 22 by amyressler@chromium.org on Wed, Mar 16, 2022, 10:32 PM EDT

Congratulations! The VRP Panel has decided to award you $7500 for this report. Thank you for your efforts and reporting this issue to us.

Comment 23 by amyressler@google.com on Thu, Mar 17, 2022, 5:29 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 24 by amyressler@chromium.org on Mon, Apr 25, 2022, 8:40 PM EDT

Labels: Release-0-M101

Comment 25 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT

Labels: CVE-2022-1484 CVE_description-missing

Comment 26 by sheriffbot on Tue, Jun 14, 2022, 1:27 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 27 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 28 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing