


☆ Starred by 4 users

Owner:

steimel@chromium.org

CC:

gov...@chromium.org
adetaylor@chromium.org
 srinivassista@chromium.org
dpa...@chromium.org

Status:

Fixed (Closed)

Components:

Internals>Media>Feeds

Modified:

Aug 19, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Android, Windows, Chrome, Mac

Pri:

1

Type:

Bug-Security

Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
M-90
Target-89
Target-90
merge-merged-4240
LTS-Security-86
external_security_report
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4430_101
Release-3-M90
CVE-2021-30508

Issue 1195340: Security: HeapOverflow in MediaFeeds

Reported by leecraso@gmail.com on Fri, Apr 2, 2021, 7:12 AM EDT

 Code

VULNERABILITY DETAILS

When making a search in `[entity_values][1]`, there is no check whether the query result is `end()`. If the author's type is not "person", `find_if()` will return `end()`. Then the `HeapOverflow` will be triggered when the `[person][2]` get accessed.

[1].
https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/media/feeds/media_feeds_converter.cc;l=503;drc=09a4396a448775456084fe36bb84662f5757d988
[2].
https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/media/feeds/media_feeds_converter.cc;l=509;drc=09a4396a448775456084fe36bb84662f5757d988

VERSION

Chrome Version: stable
Operating System: All

REPRODUCTION CASE

1. Apply the attached `https.patch` to bypass HTTPS check, or use an HTTPS server. It has nothing to do with the vulnerability itself.
2.

```
$ python -m SimpleHTTPServer  
$ out/asan/chrome --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html"
```
3. visit `chrome://media-feeds` and click "Fetch Feed" in the "Actions" column.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION

Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab

asan
50.5 KB [View](#) [Download](#)

https.patch
1.1 KB [View](#) [Download](#)

poc.html
114 bytes [View](#) [Download](#)

VideoObject
2.0 KB [View](#) [Download](#)

Comment 1 by [sheriffbot](#) on Fri, Apr 2, 2021, 7:13 AM EDT Project Member

Labels: external_security_report

Comment 2 by [drubery@chromium.org](#) on Mon, Apr 5, 2021, 1:26 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: steimel@chromium.org

Labels: Security_Severity-High Security_Impact-Stable OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1

Thanks for the report! I was able to reproduce the PoC as described. Due to the need for some unusual user gestures, triaging as High severity. If you can demonstrate the same vulnerability without having the user open chrome://media-feeds, this would be higher severity.

steimel@ - can you take a look?

Comment 3 by [sheriffbot](#) on Tue, Apr 6, 2021, 12:47 PM EDT Project Member

Labels: Target-89 M-89

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 4 by [steimel@chromium.org](#) on Wed, Apr 7, 2021, 8:05 PM EDT Project Member

Media feeds will never be fetched without the user going to chrome://media-feeds and either manually fetching one or turning on auto-fetching (which is disabled by default and can only be turned on by going to chrome://media-feeds and turning it on).

Media feeds has recently been completely deleted here: crrev.com/c/2803838

Comment 5 by [cthomp@chromium.org](#) on Fri, Apr 9, 2021, 5:14 PM EDT Project Member

Components: Internals>Media>Feeds

Sheriff here: Should we consider crrev.com/c/2803838 to be the "fix" for this then, and handle things accordingly (i.e., marking this Fixed, handling merges as needed, etc.)? Can we disable this via Finch for current release milestones?

Comment 6 by [steimel@chromium.org](#) on Fri, Apr 9, 2021, 6:10 PM EDT Project Member

We can disable the automatic fetching via Finch (which will help the case where a user has explicitly gone to chrome://media-feeds and turned on automatic fetching). The manual fetching by going to chrome://media-feeds and fetching a feed cannot be disabled via Finch. Not sure the best path forward for merging stuff back.

Comment 7 by [cthomp@chromium.org](#) on Mon, Apr 12, 2021, 12:03 PM EDT Project Member

Is manual fetching controlled by the kMediaFeeds flag? That seems (to my very brief uneducated skimming) to be the simplest thing to cherry-pick into release branches.

```
// Enables Media Feeds to allow sites to provide specific recommendations for
// users.
```

```
const base::Feature kMediaFeeds("MediaFeeds", base::FEATURE_ENABLED_BY_DEFAULT);
```

Comment 8 by [steimel@chromium.org](#) on Mon, Apr 12, 2021, 12:22 PM EDT Project Member

Yep you're right i missed that somehow. Should we cherry-pick a CL to disable that by default or just land a Finch config to disable by Finch?

Comment 9 by [cthomp@chromium.org](#) on Mon, Apr 12, 2021, 2:06 PM EDT Project Member

Cc: adetaylor@chromium.org

+adetaylor@ for help deciding merges vs. Finch config changes here.

Comment 10 by [adetaylor@chromium.org](#) on Mon, Apr 12, 2021, 8:19 PM EDT Project Member

I think we'd marginally prefer a CL to disable it in code, because of course there are some users who don't/can't access Finch, but I don't think we have a strong preference.

Comment 11 by [sheriffbot](#) on Thu, Apr 15, 2021, 12:21 PM EDT Project Member

Labels: -M-89 M-90 Target-90

Comment 12 by [leecraso@gmail.com](#) on Thu, Apr 22, 2021, 6:27 AM EDT

friendly ping

Comment 13 by [steimel@chromium.org](#) on Thu, Apr 22, 2021, 6:19 PM EDT Project Member

Status: Started (was: Assigned)

Comment 14 by [steimel@chromium.org](#) on Thu, Apr 22, 2021, 6:22 PM EDT Project Member

Do we need some sort of merge request acceptance to land the CL? There is no existing CL for trunk, since the code is gone in M91+. My goal is to land crrev.com/c/2847504

Comment 15 by [adetaylor@chromium.org](#) on Thu, Apr 22, 2021, 6:38 PM EDT Project Member

Cc: srinivassista@chromium.org gov...@chromium.org

+srinivassista, +govind as I don't know the answer.

Comment 16 by [steimel@chromium.org](#) on Tue, Apr 27, 2021, 3:32 PM EDT Project Member

friendly ping

Comment 17 by [leecraso@gmail.com](#) on Thu, Apr 29, 2021, 10:37 PM EDT

Hi, any updates?

Comment 18 by [srinivassista@google.com](#) on Fri, Apr 30, 2021, 12:34 PM EDT Project Member

Sorry for the delay, looks like this is specific merge to M90 only and cannot land on trunk for verification. I see this is only making the feature disabled, so i am assuming this to be really safe to take into M90 directly.

Only question about one of the changes. chrome/test/data/webui/media/media_feeds_webui_browsertest.js has two features enabled in the list, where as other files seem to disable/remove the list, is this intended?

Yes we do take merges to M90 directly for cases like this, as we cannot land on trunk One last question (is the code and feature flag cleaned up in M91+ ? and hence we cannot land this on trunk?)

Comment 19 by [steimel@chromium.org](#) on Fri, Apr 30, 2021, 3:25 PM EDT Project Member

Re: "Only question about one of the changes. chrome/test/data/webui/media/media_feeds_webui_browsertest.js has two features enabled in the list, where as other files seem to disable/remove the list, is this intended? ":

Yes, this is intended. I opted to go for the simplest way to get the tests working, and enabling for the test there was easiest

Re: "is the code and feature flag cleaned up in M91+ ? and hence we cannot land this on trunk?":

Yes, the code and flag are completely removed in trunk

[Comment 20](#) by [srinivassista@google.com](#) on Mon, May 3, 2021, 2:21 PM EDT Project Member

Labels: Merge-Request-90

sounds good then you can land the CL to M90 once adrian approves it, adding Merge-request-90 label

[Comment 21](#) by [adetaylor@google.com](#) on Tue, May 4, 2021, 12:57 PM EDT Project Member

Labels: -Merge-Request-90 Merge-Approved-90

Approving merge to M90, branch 4430. Please merge by EOD PST Thursday for inclusion in next week's security refresh. Please mark this as Fixed too.

[Comment 22](#) by [steimel@chromium.org](#) on Tue, May 4, 2021, 1:05 PM EDT Project Member

Cc: dpa...@chromium.org

[Comment 23](#) by [gov...@chromium.org](#) on Tue, May 4, 2021, 2:11 PM EDT Project Member

Please merge your change to M90 branch 4430 ASAP so we can pick it up for next M90 respin. Thank you.

[Comment 24](#) by [Git Watcher](#) on Tue, May 4, 2021, 3:31 PM EDT Project Member

Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+b064a73431541e520d273c227e762983c2f177b7>

commit [b064a73431541e520d273c227e762983c2f177b7](#)

Author: Tommy Steimel <steimel@chromium.org>

Date: Tue May 04 19:30:56 2021

Media Feeds: Disable Media Feeds and related features in M90

Media Feeds is deleted in M91 and later and is unused in previous versions as well. There is a security issue with Media Feeds though, so we'd like to force it to be disabled in previous versions, so this CL turns it off for M90.

[Bug-1105340](#)

Change-Id: I29e18be2abe4c1b4560d6324af3b6da93a97d947

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2847504>

Reviewed-by: dpapad <dpapad@chromium.org>

Reviewed-by: Frank Liberato <liberato@chromium.org>

Commit-Queue: Tommy Steimel <steimel@chromium.org>

Cr-Commit-Position: refs/branch-heads/4430@(#1389)

Cr-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@(#857950)

[modify] https://crrev.com/b064a73431541e520d273c227e762983c2f177b7/chrome/browser/ui/webui/chrome_url_data_manager_browsertest.cc

[modify] https://crrev.com/b064a73431541e520d273c227e762983c2f177b7/chrome/test/data/webui/media/media_feeds_webui_browsertest.js

[modify] https://crrev.com/b064a73431541e520d273c227e762983c2f177b7/chrome/test/data/webui/media/media_history_webui_browsertest.js

[modify] https://crrev.com/b064a73431541e520d273c227e762983c2f177b7/media/base/media_switches.cc

[Comment 25](#) by [adetaylor@google.com](#) on Thu, May 6, 2021, 12:13 PM EDT Project Member

steimel@ thanks! Please could you mark this as Fixed too?

[Comment 26](#) by [steimel@chromium.org](#) on Thu, May 6, 2021, 12:14 PM EDT Project Member

Status: Fixed (was: Started)

[Comment 27](#) by [sheriffbot](#) on Thu, May 6, 2021, 12:43 PM EDT Project Member

Labels: reward-topanel

[Comment 28](#) by [sheriffbot](#) on Thu, May 6, 2021, 2:02 PM EDT Project Member

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

[Comment 29](#) by [amyressler@chromium.org](#) on Fri, May 7, 2021, 5:32 PM EDT Project Member

Labels: Release-3-M90

[Comment 30](#) by [vsavu@google.com](#) on Mon, May 10, 2021, 9:17 AM EDT Project Member

Labels: LTS-Security-86 LTS-Merge-Request-86

[Comment 31](#) by [amyressler@google.com](#) on Mon, May 10, 2021, 9:53 AM EDT Project Member

Labels: CVE-2021-30508 CVE_description-missing

[Comment 32](#) by [Git Watcher](#) on Wed, May 12, 2021, 5:24 AM EDT Project Member

Labels: merge-merged-4430_101

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+b255003117360100eb7c79f9caedf54ddda9fcd>

commit [b255003117360100eb7c79f9caedf54ddda9fcd](#)

Author: Tommy Steimel <steimel@chromium.org>

Date: Wed May 12 09:22:21 2021

Media Feeds: Disable Media Feeds and related features in M90

Media Feeds is deleted in M91 and later and is unused in previous versions as well. There is a security issue with Media Feeds though, so we'd like to force it to be disabled in previous versions, so this CL turns it off for M90.

(cherry picked from commit [b064a73431541e520d273c227e762983c2f177b7](#))

[Bug-1105340](#)

Change-Id: I29e18be2abe4c1b4560d6324af3b6da93a97d947

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2847504>

Reviewed-by: dpapad <dpapad@chromium.org>

Reviewed-by: Frank Liberato <liberato@chromium.org>

Commit-Queue: Tommy Steimel <steimel@chromium.org>

Cr-Original-Commit-Position: refs/branch-heads/4430@(#1389)

Cr-Original-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@(#857950)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2884070>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@(#22)
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@(#1364)
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@(#857950)

[modify] https://crrev.com/b255003117360100eb7c79f9caedf54ddda9fcd/chrome/browser/ui/webui/chrome_url_data_manager_browsertest.cc
[modify] https://crrev.com/b255003117360100eb7c79f9caedf54ddda9fcd/chrome/test/data/webui/media/media_feeds_webui_browsertest.js
[modify] https://crrev.com/b255003117360100eb7c79f9caedf54ddda9fcd/chrome/test/data/webui/media/media_history_webui_browsertest.js
[modify] https://crrev.com/b255003117360100eb7c79f9caedf54ddda9fcd/media/base/media_switches.cc

[Comment 33](#) by [gianluca@google.com](#) on Wed, May 12, 2021, 12:34 PM EDT Project Member
Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

[Comment 34](#) by [Git Watcher](#) on Wed, May 12, 2021, 3:05 PM EDT Project Member
Labels: merge-merged-4240

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+b45be0604d27b3e644978e57f581e810a65edca5>

commit [b45be0604d27b3e644978e57f581e810a65edca5](#)
Author: Tommy Steinel <steinel@chromium.org>
Date: Wed May 12 19:03:44 2021

Media Feeds: Disable Media Feeds and related features in M90

Media Feeds is deleted in M91 and later and is unused in previous versions as well. There is a security issue with Media Feeds though, so we'd like to force it to be disabled in previous versions, so this CL turns it off for M90.

(cherry picked from commit [b064a73431541e520d273c227e762983c2f177b7](#))

[Bug-1106340](#)

Change-Id: I29e18be2abe4c1b4560d6324af3b6da93a97d947
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2847504>
Reviewed-by: dpapad <dpapad@chromium.org>
Reviewed-by: Frank Liberato <liberato@chromium.org>
Commit-Queue: Tommy Steinel <steinel@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@(#1389)
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@(#857950)
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2883741>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@(#1639)
Cr-Branched-From: I297677702651916bbf65e59c0d4dbd4ce57d1ee-refs/heads/master@(#800218)

[modify] https://crrev.com/b45be0604d27b3e644978e57f581e810a65edca5/chrome/browser/ui/webui/chrome_url_data_manager_browsertest.cc
[modify] https://crrev.com/b45be0604d27b3e644978e57f581e810a65edca5/chrome/test/data/webui/media/media_feeds_webui_browsertest.js
[modify] https://crrev.com/b45be0604d27b3e644978e57f581e810a65edca5/chrome/test/data/webui/media/media_history_webui_browsertest.js
[modify] https://crrev.com/b45be0604d27b3e644978e57f581e810a65edca5/media/base/media_switches.cc

[Comment 35](#) by [amyressler@google.com](#) on Wed, May 12, 2021, 7:11 PM EDT Project Member
Labels: -reward-topanel reward-unpaid reward-15000

*** 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 36](#) by [amyressler@chromium.org](#) on Wed, May 12, 2021, 7:20 PM EDT Project Member
Congratulations, Leecraso and Guang Gong! The VRP Panel has decided to award you \$15,000 for this report. Excellent work!

[Comment 37](#) by [amyressler@google.com](#) on Mon, May 17, 2021, 2:24 PM EDT Project Member
Labels: -reward-unpaid reward-inprocess

[Comment 38](#) by [amyressler@google.com](#) on Fri, Jun 4, 2021, 7:23 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

[Comment 39](#) by [sheriffbot](#) on Thu, Aug 19, 2021, 1:30 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