Starred by 2 users

Owner: petermarshall@chromium.org

CC: noel@chromium.org
simmonsjosh@google.com
fdegros@chromium.org
austinct@chromium.org
lucmult@chromium.org
joelhockey@chromium.org
majewski@chromium.org
adanilo@chromium.org
jboulic@chromium.org

Status: Fixed *(Closed)*

Components: Platform>Apps>FileManager

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Chrome

Pri: 1

Type: Bug-Security

reward-10000
Security_Severity-Medium
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-97
external_security_report
Target-94
Target-93
FoundIn-93
CrOSFilesCategory-Triaged
Security_Impact-Extended
Merge-NA-97
Release-0-M97
CVE-2022-0107

Issue 1248438: uaf in FileManagerPrivateInternalComputeChecksumFunction::Run

Reported by wxhu...@gmail.com on Fri, Sep 10, 2021, 11:36 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36

Steps to reproduce the problem:
- in this private extension function FileManagerPrivateInternalComputeChecksumFunction::Run

```c++
FileManagerPrivateInternalComputeChecksumFunction::Run() {
  using drive::util::FileStreamMd5Digester;
  using extensions::api::file_manager_private_internal::ComputeChecksum::Params;
  const std::unique_ptr<Params> params(Params::Create(args()));
  EXTENSION_FUNCTION_VALIDATE(params);

  if (params->url.empty()) {
    return RespondNow(Error("File URL must be provided."));
  }

  scoped_refptr<storage::FileSystemContext> file_system_context =
      file_manager::util::GetFileSystemContextForRenderFrameHost(
          Profile::FromBrowserContext(browser_context()), render_frame_host());

  FileSystemURL file_system_url(
      file_system_context->CrackURLInFirstPartyContext(GURL(params->url)));
  if (!file_system_url.is_valid()) {
    return RespondNow(Error("File URL was invalid"));
  }

  std::unique_ptr<storage::FileStreamReader> reader =
      file_system_context->CreateFileStreamReader(
          file_system_url, 0, storage::kMaximumLength, base::Time());

  FileStreamMd5Digester::ResultCallback result_callback = base::BindOnce(
      &ComputeChecksumRespondOnUIThread,
      base::BindOnce(
          &FileManagerPrivateInternalComputeChecksumFunction::RespondWith,
          this));
  content::GetIOThreadTaskRunner({})->PostTask(
      FROM_HERE, base::BindOnce(&FileStreamMd5Digester::GetMd5Digest,
                                base::Unretained(digester_.get()),
                                std::move(reader), std::move(result_callback)));

  return RespondLater();
}
```

here use the io thread to post task and send the raw_pointer
```base::Unretained(digester_.get()) ``` and don't have other check.
it may cause race uaf in io thread of the private extension api
```

it may cause race uaf in io thread of the private extension api.

I don't have a poc, just code inspection.

What is the expected behavior?

What went wrong?
above all.

Did this work before? N/A

Chrome version: 93.0.4577.63 Channel: stable
OS Version: 10.0

Comment 1 by sheriffbot on Fri, Sep 10, 2021, 11:40 AM EDT

Labels: external_security_report

Comment 2 by adetaylor@google.com on Fri, Sep 10, 2021, 12:33 PM EDT

Owner: amistry@chromium.org
Cc: adanilo@chromium.org austinct@chromium.org dats@chromium.org fdegros@chromium.org jboulic@chromium.org joelhockey@chromium.org lucmult@chromium.org majewski@chromium.org noel@chromium.org simmonsjosh@google.com
Labels: -OS-Windows FoundIn-93 Security_Severity-High OS-Chrome Pri-1
Components: Platform>Apps>FileManager

Thanks for the report!

Security sheriff: This looks like it's probably a real issue to me. I can't see anything which would extend the lifetime of the ref-counted ExtensionFunction subclass such that the digester_ is guaranteed to exist that long. I might be missing something, but I'm going to pass it through to the engineering team to have a look.

Severity: browser process use-after-free => critical. Presumably requires an extension to be installed => mitigated to High severity. I'm not sure whether this code corresponds to truly private extension APIs, but if this code is accessible only from code-signed ChromeOS extensions, we can further bump it down to Medium.

FoundIn => it looks like the relevant code hasn't changed lately, so setting a FoundIn corresponding to the current stable branch.

Comment 3 Deleted

Comment 4 by adetaylor@google.com on Fri, Sep 10, 2021, 12:34 PM EDT

Labels: -FoundIn-92

Comment 5 by sheriffbot on Fri, Sep 10, 2021, 12:34 PM EDT

Labels: Security_Impact-Stable

Comment 6 by sheriffbot on Fri, Sep 10, 2021, 12:47 PM EDT

Labels: M-93 Target-93

Setting milestone and target because of high severity.

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

Comment 7 by sheriffbot on Fri, Sep 10, 2021, 2:22 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 8 by sheriffbot on Fri, Sep 10, 2021, 2:22 PM EDT

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 9 by simmonsjosh@google.com on Sun, Sep 12, 2021, 7:28 PM EDT

Owner: petermarshall@chromium.org
Cc: -dats@chromium.org

Re c#2: "but if this code is accessible only from code-signed ChromeOS extensions, we can further bump it down to Medium."

fileManagerPrivate is an API that is only made available to the Chrome OS File Manager Chrome App (usages: [1]), so I think we can bump severity down to Medium. If anyone disagrees, please change back to High.

The only usage of this API function appears to be from here [2] and that JS class doesn't actually look to be used at all [3]. I think we can remove both the JS class and the corresponding C++ implementation.

petermarshall@ WDYT?

[1] https://source.chromium.org/search?q=fileManagerPrivate%20f:json&start=1
[2] https://source.chromium.org/chromium/chromium/src/+/main:ui/file_manager/file_manager/background/js/duplicate_finder.js;l=70?q=f:ui%2Ffile_manager%20computeChecksum
[3] https://source.chromium.org/search?q=f:ui%2Ffile_manager%20DriveDuplicateFinder%20-f:out

Comment 10 by simmonsjosh@google.com on Sun, Sep 12, 2021, 7:28 PM EDT

Labels: -Security_Severity-High Security_Severity-Medium

Comment 11 by petermarshall@chromium.org on Sun, Sep 12, 2021, 8:36 PM EDT

Mm it was introduced here [1] and worked at the time I think, then years of migrations seem to have broken it.
It was a temporary fix anyway apparently.
I will go ahead and remove it

[1] https://codereview.chromium.org/840843002/diff/60001/chrome/browser/chromeos/extensions/file_manager/private_api_file_system.cc

Comment 12 by lucmult@chromium.org on Sun, Sep 12, 2021, 9:14 PM EDT

The code seems to be used here [1].

There are 2 UMAs from that code too:
https://screenshot.googleplex.com/Qgy8QWsPh8TqSeR
https://screenshot.googleplex.com/zC2gjgeNsaAay42

[1] -

https://source.chromium.org/chromium/chromium/src/+/main:ui/file_manager/file_manager/background/js/duplicate_finder.js;l=281;drc=86fc2702ab96e01c2a9b907ca583abdcce4f0f33

Comment 13 by petermarshall@chromium.org on Sun, Sep 12, 2021, 10:24 PM EDT

Nice find Luc. What is the lifetime of FileManagerPrivateInternalComputeChecksumFunction then?
We post the task to the IO thread and call back through ::RespondWith(), also passing a `this` pointer.
So I suspect that ExtensionFunctions live at least until RespondWith() is called, meaning digester_ stays alive at least until the IO thread calls back after it is done with FileStreamMd5Digester::GetMd5Digest.

Comment 14 by wxhu...@gmail.com on Mon, Sep 13, 2021, 3:54 AM EDT

from this link,
https://source.chromium.org/chromium/chromium/src/+/main:extensions/browser/extension_function.cc;l=417;drc=a9641800e0e8f7a2ea9a5f55f831b632e990a0e0
it seems that
```
ExtensionFunction::~ExtensionFunction() {
  if (name())  // name_ may not be set in unit tests.
    ExtensionFunctionMemoryDumpProvider::GetInstance().RemoveFunctionName(
        name());
  if (dispatcher() && (render_frame_host() || is_from_service_worker())) {
    dispatcher()->OnExtensionFunctionCompleted(
        extension(), is_from_service_worker(), name());
  }

// The extension function should always respond to avoid leaks in the
// renderer, dangling callbacks, etc. The exception is if the system is
// shutting down or if the extension has been unloaded.
#if DCHECK_IS_ON()
  auto can_be_destroyed_before_responding = [this]() {
    extensions::ExtensionsBrowserClient* browser_client =
        extensions::ExtensionsBrowserClient::Get();
    if (!browser_client || browser_client->IsShuttingDown())
      return true;
```

Comment 15 by wxhu...@gmail.com on Mon, Sep 13, 2021, 4:04 AM EDT

this exception seems special and maybe cause a wider problem?

Comment 16 by austinct@chromium.org on Mon, Sep 13, 2021, 11:33 PM EDT

Labels: CrOSFilesCategory-Triaged

Comment 17 by sheriffbot on Wed, Sep 22, 2021, 12:21 PM EDT

Labels: -M-93 Target-94 M-94

Comment 18 by sheriffbot on Mon, Sep 27, 2021, 12:21 PM EDT

petermarshall: 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?

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 19 by lucmult@chromium.org on Wed, Oct 6, 2021, 11:35 PM EDT

I've given some thought to this, reading our docs about callback [1].

The core issue here is because we're using `base::Unretained()` in [2] and [3]. The doc [1] says we should use RefCounted type for this or WeakPtr. Probably changing FileStreamMd5Digester to be refcounted, this class is only used in one place, so shouldn't be too complicated.

```
By default the object must support RefCounted or you will get a compiler error. If you're passing between threads, be sure it's RefCountedThreadSafe!
```

[1] - https://source.chromium.org/chromium/chromium/src/+/main:docs/callback.md
[2] - https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/chromeos/extensions/file_manager/private_api_file_system.cc;l=1133;drc=2ed65483549494f999d6389bde19b98693af6a27
[3] - https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/chromeos/extensions/file_manager/file_stream_md5_digester.cc;l=46;drc=1bbf8ac9caa7e57a52a71deec56bf1b6f683c6bd

Comment 20 by petermarshall@chromium.org on Thu, Oct 7, 2021, 6:44 PM EDT

Status: Started (was: Assigned)

Comment 21 by simmonsjosh@google.com on Sun, Oct 10, 2021, 6:56 PM EDT

Labels: -M-94 M-97

Comment 22 by Git Watcher on Mon, Oct 11, 2021, 9:49 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6fbc440cbe7f71e88170624b2fa76470d0cc4885

commit 6fbc440cbe7f71e88170624b2fa76470d0cc4885
Author: Peter Marshall <petermarshall@chromium.org>
Date: Tue Oct 12 01:48:55 2021

Change FileStreamMd5Digester to refcounted

~~Bug: 1248438~~
Change-Id: I04d6ae5018da152713bddada2c5fc666223bb424

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3211408
Reviewed-by: Luciano Pacheco <lucmult@chromium.org>
Commit-Queue: Peter Marshall <petermarshall@chromium.org>

Commit-Queue: Peter Marshall <petermarshall@chromium.org>
Cr-Commit-Position: refs/heads/main@{#930372}

[modify]
https://crrev.com/6fbc440cbe7f71e88170624b2fa76470d0cc4885/chrome/browser/chromeos/extensions/file_manager/private_api_file_system.cc
[modify]
https://crrev.com/6fbc440cbe7f71e88170624b2fa76470d0cc4885/chrome/browser/chromeos/extensions/file_manager/file_stream_md5_digester.cc
[modify]
https://crrev.com/6fbc440cbe7f71e88170624b2fa76470d0cc4885/chrome/browser/chromeos/extensions/file_manager/file_stream_md5_digester.h
[modify]
https://crrev.com/6fbc440cbe7f71e88170624b2fa76470d0cc4885/chrome/browser/chromeos/extensions/file_manager/private_api_file_system.h

Comment 23 by petermarshall@chromium.org on Mon, Oct 25, 2021, 11:16 PM EDT

Status: Fixed (was: Started)

Comment 24 by sheriffbot on Tue, Oct 26, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 25 by sheriffbot on Tue, Oct 26, 2021, 1:41 PM EDT

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

Comment 26 by amyressler@google.com on Wed, Nov 3, 2021, 1:53 PM EDT

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 27 by amyressler@chromium.org on Wed, Nov 3, 2021, 2:23 PM EDT

Congratulations! The VRP Panel has decided to award you $10,000 for this report. Nice work!!

Comment 28 by amyressler@google.com on Thu, Nov 4, 2021, 4:31 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 29 by sheriffbot on Sun, Nov 7, 2021, 2:16 PM EST

Labels: Merge-NA-97

Not requesting merge to dev (M97) because latest trunk commit (930372) appears to be prior to dev branch point (938553).

If this is incorrect, please replace the Merge-NA-97 label with Merge-Request-97. If other changes are required to fix this bug completely, please request a merge if necessary.

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

Comment 30 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:30 PM EST

Labels: Release-0-M97

Comment 31 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST

Labels: CVE-2022-0107 CVE_description-missing

Comment 32 by sheriffbot on Tue, Feb 1, 2022, 1:30 PM EST

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 33 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT

Labels: -CVE_description-missing CVE_description-submitted