bugs chromium ▾ New issue Open issues ▾ Search chromium issue ▾ Sign in

☆ Starred by 3 users

Owner:	ericwilligers@chromium.org
CC:	mho...@microsoft.com jsb...@chromium.org mthiesse@chromium.org mgiuca@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebShare
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-88
external_security_report
M-98
Target-98
Security_Impact-Extended
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1128

Issue 1301920: Security: Web Share API allows to write in UNC paths and/or in C:/Users/<username>/AppData/Local/Temp/ on Windows

Reported by maury...@gmail.com on Tue, Mar 1, 2022, 6:32 AM EST

Code

VULNERABILITY DETAILS

The Web Share API, which is enabled on Chrome for Windows, allows what follows:

- When a `files` attribute is present and the `share` function is invoked, the `files` are stored with an arbitrary filename in `C:/Users/<username>/AppData/Local/Temp/` without notifying the user that a download started.
- When a `files` attribute is present, the `share` function is invoked, and the name of one of the `files` is an UNC path, then Windows connects to such UNC path (if a SMB server is exposed then it leaks the NetNTLMv2 hashes, if it is not exposed it tries to perform a WebDAV connection).

Note that the filenames are not 100% arbitrary as there is an extensions allow-list defined here: https://developer.mozilla.org/en-US/docs/Web/API/Navigator/share#shareable_file_types

In case your are not into Windows' authentication mechanisms basically when Windows tries to connect to a SMB share it send the current user password hash in the NetNTLMv2 format. Such hash could be relayed to another Windows computer the user has access to or the attacker could crack it offline to obtain the user's cleartext password.

VERSION

Chrome Version: 98.0.4758.102 stable
Operating System: Microsoft Windows 11 - 10.0.22000 Build 22000

REPRODUCTION CASE

1. Create an HTTP server
2. Create a SMB server with [Responder.py](https://github.com/SpiderLabs/Responder) (i.e. `sudo ./Responder.py -w -I <network_interface_name>`)
3. Host the attached HTML PoC files on the HTTP server created at step 1
4. Replace in the `webshare_poc2.html` the 10th line with the SMB server IP address created at step 2
5. Open the file browser of the Windows client in `C:/Users/<username>/AppData/Local/Temp/`
6. Notice that a file called `00_written.html` does not exist
7. Visit `webshare_poc1.html` in Chrome
8. Click the `SHARE` button
9. Open again the file browser of the Windows client in `C:/Users/<username>/AppData/Local/Temp/`
10. Notice that `00_written.html` has been written
11. Visit `webshare_poc2.html` in Chrome
12. Click the `SHARE` button
13. Notice in Responder that a new SMB request has been received with the NetNTLMv2 hashes of the victim

CREDIT INFORMATION

Reporter credit: Abdel Adim [`smaury`](https://twitter.com/smaury92) Oisfi of [Shielder](https://www.shielder.it)

webshare_poc1.html
769 bytes View Download

webshare_poc2.html
928 bytes View Download

Comment 1 by sheriffbot on Tue, Mar 1, 2022, 6:35 AM EST Project Member

Labels: external_security_report

Comment 2 by maury...@gmail.com on Tue, Mar 1, 2022, 10:27 AM EST

As far as I understood by reading the code, the bug should be here in `ShareOperation::PutShareContentInDataPackage` (https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/win/share_operation.cc#508).

Here (https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/win/share_operation.cc#563) all the `file` in `files` are read and stored to the filesystem using the `windows.storage` class.

Precisely, the filename is read here (https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/win/share_operation.cc#576) and used as argument of the `CreateStreamedFileAsync` function here (https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/win/share_operation.cc#594).

Comment 3 by dcheng@chromium.org on Thu, Mar 3, 2022, 5:56 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: ericwilligers@chromium.org
Cc: mho...@microsoft.com
Labels: Security_Severity-Low FoundIn-88 OS-Chrome OS-Mac OS-Windows OS-Lacros Pri-2
Components: Blink>WebShare

Hmm... so if I understand correctly, it looks like this is allowing a page to provide absolute paths for sharing? That sounds unintended and not ideal. I tested with a simple poc that doesn't require a UNC path and just specified a random absolute path, and verified that I see an attempt to open a file at that absolute path in process monitor.

Possible solution here is to use mojo_base.mojom.SafeBaseName, which among other things, ensures that we don't have an absolute path or a path component that tries to perform directory traversal.

I don't /think/ this should be an info leak though; I wasn't able to trigger share (at least on Windows) to leak the contents of the file at the absolute path (I got a dialog that says "Try that again: We couldn't show you all the ways you could share"), nor was I able to convince Chrome to overwrite the file with arbitrary contents.

Given that, I think this is a low severity bug, but I did not attempt to examine all platform implementations.

Tagging this with M88 since that's when the Windows implementation was introduced:
https://chromium.googlesource.com/chromium/src.git/+/e790f0c81dc63334a8b5429a04a34be6e571467a

Tagging this with all the OSes that I believe webshare is implemented on, based on
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/webshare/share_service_impl.cc;l=251;drc=d8a6d8ffe9f0985574752fa33b81358ef48c4cfc

Comment 4 by sheriffbot on Thu, Mar 3, 2022, 6:00 PM EST Project Member

Labels: Security_Impact-Extended

Comment 5 by maury...@gmail.com on Thu, Mar 3, 2022, 6:29 PM EST

Hi dcheng@,
I strongly advise you to reproduce it with an UNC path and Responder to better see the security impact.

Basically that way you don't leak the file content, which is not really interesting in this context, but you leak the hash of the Windows user password.

Seeing the "Try that again: We couldn't show you all the ways you could share" is correct as it fails to write the file, on the other hand the connection to the SMB share is performed and the credentials leaked.

This could be abused to relay the NetNTLMv2 hashes (i.e. in a common Active Directory environment you could try to relay the hash to a server which has SMB signing disabled and abuse the victim's credentials).

I would consider this as a partial SOP bypass too as you can trigger an interaction to an UNC path (which is in the file:// context) from a web page (in the https:// context).

So probably raising to Security_Severity-High is more appropriate, just my 2 cents obviously.

Comment 6 by ericwilligers@chromium.org on Thu, Mar 3, 2022, 6:36 PM EST Project Member

Status: Started (was: Assigned)

Comment 7 by mho...@microsoft.com on Thu, Mar 3, 2022, 7:29 PM EST Project Member

For some context on at least part of this - the Windows API being used (CreateStreamedFileAsync) is intended for creating a virtual file that does not *have to* live on disk. It is up to Windows to decide if, when, where, and under what name to create an actual file to store the data given to it. When it does decide to make a file it does appear to do so by default in the user's %temp% directory, starting with the originally provided name and only modifying the name if there is a naming collision. (Side note - the virtual file's name is not impacted by the name Windows decides to give to the actual file)

Given how that portion works, I would not expect it to ever overwrite an existing file, or surface the data of an existing file - though it may be checking if an absolute file path exists when it probably shouldn't be, since it won't be creating a file in that location. That same code sounds like it may also be 'checking' UNC paths, which sounds like the biggest issue here.

Comment 8 by ericwilligers@chromium.org on Thu, Mar 3, 2022, 7:59 PM EST Project Member

The renderer can discard everything before the final \ or / , e.g. by using SafeBaseName.

I'm not sure how to create a WTF::String from a base::SafeBaseName and I don't have a Windows machine at home. Currently I'm instead working on a change to the mojom:

```
struct SharedFile {
  SafeBaseName name;
  SerializedBlob blob;
};
```

This will require code changes in the Android/ChromeOS/Mac/Windows browser code.

Comment 9 by ericwilligers@chromium.org on Fri, Mar 4, 2022, 1:37 AM EST Project Member

In-progress mojom change:
https://chromium-review.googlesource.com/c/chromium/src/+/3503074

Comment 10 by maury...@gmail.com on Fri, Mar 4, 2022, 1:51 AM EST

I had a quick look to the Android/ChromeOS/Mac implementations and when it comes to handling the file->name param they behave differently, namely they are either using a random-ish name or they are sanitising the name right before saving it to disk.

Mac: It sanitises the file->name here:
https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/mac/sharing_service_operation.mm#128

128
ChromeOS: It generates a random-sh filename using the net::GenerateFileName function here:
https://chromium.googlesource.com/chromium/src/+/main/chrome/browser/webshare/chromeos/sharesheet_client.cc#223
Android: It generate a random-ish filename using the File.createTempFile function here:
https://chromium.googlesource.com/chromium/src/+/refs/heads/main/components/browser_ui/webshare/android/java/src/org/chromium/components/browser_ui/webshare/ShareServiceImpl.java#249

So *maybe* implementing something similar in Windows could be the easiest solution?

Comment 11 by dcheng@chromium.org on Fri, Mar 4, 2022, 2:39 AM EST Project Member

Labels: -OS-Chrome -OS-Mac -OS-Lacros Security_Severity-Critical Pri-0

> This could be abused to relay the NetNTLMv2 hashes (i.e. in a common Active Directory environment you could try to relay the hash to a server which has SMB signing disabled and abuse the victim's credentials).

Sorry, I chatted with a few Windows people right after I posted the first update and didn't get a chance to return to updating this bug until now. What I wanted to confirm with them is if this would leak hashes to any random domain on the internet. It seems like it would. So based purely on this, I think this is actually critical or high severity. I'm going to set critical for now :)

As for the other point about this being a SOP bypass--sort of but not really. It is making requests it's not supposed to be able to, but I also don't know of a way to turn this into a XSRF. But if you know of a way this would allow XSRF, that would be an interesting addition to mention.

> I'm not sure how to create a WTF::String from a base::SafeBaseName

You can do something like blink::FilePathToString(safe_name.path()) to go base::SafeBaseName -> WTF::String.

> So *maybe* implementing something similar in Windows could be the easiest solution?

This would be one approach, but it wouldn't be the preferred approach. Using the correct underlying type prevents future implementations from potentially suffering the same issues.

> I had a quick look to the Android/ChromeOS/Mac implementations and when it comes to handling the file->name param they behave differently, namely they are either using a random-ish name or they are sanitising the name right before saving it to disk.

Thanks, that does help narrow down the affected platforms.

Comment 12 by ericwilligers@chromium.org on Fri, Mar 4, 2022, 7:41 AM EST Project Member

Cc: jsb...@chromium.org

Comment 13 by sheriffbot on Fri, Mar 4, 2022, 12:47 PM EST Project Member

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 14 by sheriffbot on Fri, Mar 4, 2022, 1:24 PM EST Project Member

Labels: -Pri-0 Pri-2

Setting Pri-2 to match security severity Low. 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 dcheng@chromium.org on Fri, Mar 4, 2022, 3:58 PM EST Project Member

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

After some further discussion, we'll bucket this as high.

Leaking NTLM hashes doesn't seem great; at the same time, reusing passwords (or having a weak password) that can be bruteforced is kind of a recipe for disaster.

Fixing the severity labels to unconfuse sheriffbot too.

Comment 16 by maury...@gmail.com on Fri, Mar 4, 2022, 6:39 PM EST

> Leaking NTLM hashes doesn't seem great; at the same time, reusing passwords (or having a weak password) that can be bruteforced is kind of a recipe for disaster.

Something which should be taken in account is that the password cracking is not the only option for an attacker, in fact when it comes to NetNTLMv2 you could still relay the hash without cracking it (I really suggest reading this guide which describes how this attack is still relevant in 2022: https://www.trustedsec.com/blog/a-comprehensive-guide-on-relaying-anno-2022/). This is a *very common* TTP (Tools Tactics and Procedures) used to attack Windows devices in Active Directory environments (so basically the most common setup in the companies).

> After some further discussion, we'll bucket this as high.

I would still consider this as critical / Pri-0 based on the relaying attack scenario, again just my 2 cents.

Comment 17 by Git Watcher on Tue, Mar 8, 2022, 10:45 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/26f39eab6cefe74baef3b0451b63cadd6a7eb84c

commit 26f39eab6cefe74baef3b0451b63cadd6a7eb84c
Author: Eric Willigers <ericwilligers@chromium.org>
Date: Tue Mar 08 15:44:00 2022

Web Share API: Use SafeBaseName

We update mojom struct SharedFile to use SafeBaseName.

A new Android test shows '/' is rejected as a Web Share filename.

~~Bug: 1301920~~

Change-Id: Ic49117dab8cbc6a689a8b83b1c39409725f96cb8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503074
Reviewed-by: Michael Thiessen <mthiesse@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Eric Willigers <ericwilligers@chromium.org>
Auto-Submit: Eric Willigers <ericwilligers@chromium.org>
Cr-Commit-Position: refs/heads/main@{#978724}

[modify]
https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/share_service_unittest.cc

https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/share_service_unittest.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/chromeos/sharesheet_client_browsertest.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/ui/web_applications/web_share_target_browsertest.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/third_party/blink/renderer/modules/webshare/navigator_share_test.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/chromeos/sharesheet_client.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/mac/sharing_service_operation.mm
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/third_party/blink/public/mojom/webshare/webshare.mojom
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/chromeos/sharesheet_client_unittest.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/android/BUILD.gn
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/components/browser_ui/webshare/android/BUILD.gn
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/win/share_operation_unittest.cc
[add] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/third_party/blink/renderer/modules/webshare/DEPS
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/share_service_impl.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/win/share_operation.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/android/javatests/src/org/chromium/chrome/browser/webshare/WebShareTest.java
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/third_party/blink/tools/blinkpy/presubmit/audit_non_blink_usage.py
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/test/data/webshare/index.html
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/third_party/blink/renderer/modules/webshare/navigator_share.cc
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/chrome/browser/webshare/share_service_impl.h
[add] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/content/test/data/android/webshare-separator.html
[modify] https://crrev.com/26f39eab6cefe74baef3b0451b63cadd6a7eb84c/components/browser_ui/webshare/android/java/src/org/chromium/components/browser_ui/webshare/ShareServiceImpl.java

Comment 18 by Git Watcher on Tue, Mar 8, 2022, 4:56 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/fcb2ea2c4676f96921b067bf7da192a0692c2215

commit fcb2ea2c4676f96921b067bf7da192a0692c2215
Author: Eric Willigers <ericwilligers@chromium.org>
Date: Tue Mar 08 21:55:02 2022

Update SharingServiceOperationBrowserTest

The expectation was failing on mac11-arm64-rel-tests
after crrev.com/c/3503074 (using BaseFilename in Web Share mojom).

~~Bug: 1304291~~,~~1301920~~
Change-Id: Ic1d72ccd52026986ba5d4c185cc38422c063b9e2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3511227
Commit-Queue: Eric Willigers <ericwilligers@chromium.org>
Auto-Submit: Eric Willigers <ericwilligers@chromium.org>
Reviewed-by: Dominique Fauteux-Chapleau <domfc@chromium.org>
Commit-Queue: Dominique Fauteux-Chapleau <domfc@chromium.org>
Cr-Commit-Position: refs/heads/main@{#978886}

[modify] https://crrev.com/fcb2ea2c4676f96921b067bf7da192a0692c2215/chrome/browser/webshare/mac/sharing_service_operation_browsertest.cc

Comment 19 by ericwilligers@chromium.org on Tue, Mar 8, 2022, 5:18 PM EST Project Member

Status: Fixed (was: Started)

Comment 20 by sheriffbot on Wed, Mar 9, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 21 by sheriffbot on Wed, Mar 9, 2022, 1:42 PM EST Project Member

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

Comment 22 by sheriffbot on Wed, Mar 9, 2022, 2:02 PM EST Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (978886) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (978886) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (978886) appears to be after beta branch point (972766).

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

Comment 23 by sheriffbot on Wed, Mar 9, 2022, 2:08 PM EST Project Member

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

Merge review required: a commit with DEPS changes was detected.

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: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 24 by sheriffbot on Wed, Mar 9, 2022, 2:08 PM EST Project Member

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

Merge review required: a commit with DEPS changes was detected.

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), ceb (ChromeOS), pbommana (Desktop)

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

Comment 25 by sheriffbot on Wed, Mar 9, 2022, 2:08 PM EST Project Member

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

Merge review required: a commit with DEPS changes was detected.

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 26 by ericwilligers@chromium.org on Wed, Mar 9, 2022, 4:39 PM EST Project Member

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

Chrome Browser:
Yes: Security_Severity-High

Chrome OS:
No need for additional Chrome OS merges - this is a Windows issue.

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

https://chromium-review.googlesource.com/c/chromium/src/+/3503074
https://chromium-review.googlesource.com/c/chromium/src/+/3511227

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

Yes. 101.0.4933.0

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

N/A.

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.

No.

Comment 27 by srinivassista@google.com on Thu, Mar 10, 2022, 12:00 PM EST Project Member

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

Merge approved M100 branch:pls refer to go/chrome-branches for branch info

Comment 28 by ericwilligers@chromium.org on Thu, Mar 10, 2022, 2:11 PM EST Project Member

Cc: mthiesse@chromium.org

Comment 29 by ericwilligers@chromium.org on Thu, Mar 10, 2022, 3:24 PM EST Project Member

Merging to M100 in crrev.com/c/3517925 crrev.com/c/3517926

Comment 30 by Git Watcher on Thu, Mar 10, 2022, 4:30 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4751620d00b41155bbfb791111583f6ae8bb19e8

commit 4751620d00b41155bbfb791111583f6ae8bb19e8
Author: Eric Willigers <ericwilligers@chromium.org>
Date: Thu Mar 10 21:29:07 2022

Web Share API: Use SafeBaseName

We update mojom struct SharedFile to use SafeBaseName.

A new Android test shows '/' is rejected as a Web Share filename.

~~Bug: 1301920~~

(cherry picked from commit 26f39eab6cefe74baef3b0451b63cadd6a7eb84c)

Change-Id: Ic49117dab8cbc6a689a8b83b1c39409725f96cb8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503074
Reviewed-by: Michael Thiessen <mthiesse@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Eric Willigers <ericwilligers@chromium.org>
Auto-Submit: Eric Willigers <ericwilligers@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#978724}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3517925
Reviewed-by: Eric Willigers <ericwilligers@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Daniel Cheng <dcheng@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#449}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/share_service_unittest.cc
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/chromeos/sharesheet_client_browsertest.cc
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/ui/web_applications/web_share_target_browsertest.cc
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/renderer/modules/webshare/navigator_share_test.cc
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/chromeos/sharesheet_client.cc
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/mac/sharing_service_operation.mm
[modify]
https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/public/mojom/webshare/webshare.mojo

https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/public/mojom/webshare/webshare.mojom
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/chromeos/sharesheet_client_unittest.cc
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/android/BUILD.gn
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/components/browser_ui/webshare/android/BUILD.gn
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/win/share_operation_unittest.cc
[add] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/renderer/modules/webshare/DEPS
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/share_service_impl.cc
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/win/share_operation.cc
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/tools/blinkpy/presubmit/audit_non_blink_usage.py
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/android/javatests/src/org/chromium/chrome/browser/webshare/WebShareTest.java
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/test/data/webshare/index.html
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/chrome/browser/webshare/share_service_impl.h
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/third_party/blink/renderer/modules/webshare/navigator_share.cc
[add] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/content/test/data/android/webshare-separator.html
[modify] https://crrev.com/4751620d00b41155bbfb791111583f6ae8bb19e8/components/browser_ui/webshare/android/java/src/org/chromium/components/browser_ui/webshare/ShareServiceImpl.java

Comment 31 by Git Watcher on Thu, Mar 10, 2022, 5:14 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0c06be8f0f33fbdc856018b45e7d71bcb78385e4

commit 0c06be8f0f33fbdc856018b45e7d71bcb78385e4
Author: Eric Willigers <ericwilligers@chromium.org>
Date: Thu Mar 10 22:13:37 2022

Update SharingServiceOperationBrowserTest

The expectation was failing on mac11-arm64-rel-tests
after crrev.com/c/3503074 (using BaseFilename in Web Share mojom).

(cherry picked from commit fcb2ea2c4676f96921b067bf7da192a0692c2215)

~~Bug: 1304291~~,~~1301920~~
Change-Id: Ic1d72ccd52026986ba5d4c185cc38422c063b9e2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3511227
Commit-Queue: Eric Willigers <ericwilligers@chromium.org>
Auto-Submit: Eric Willigers <ericwilligers@chromium.org>
Reviewed-by: Dominique Fauteux-Chapleau <domfc@chromium.org>
Commit-Queue: Dominique Fauteux-Chapleau <domfc@chromium.org>

Commit-Queue: Dominique Fauteux-Chapleau <domfc@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#978886}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3517926
Reviewed-by: Eric Willigers <ericwilligers@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@{#450}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify] https://crrev.com/0c06be8f0f33fbdc856018b45e7d71bcb78385e4/chrome/browser/webshare/mac/sharing_service_operation_browsertest.cc

Comment 32 by amyressler@google.com on Wed, Mar 16, 2022, 9:46 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 33 by amyressler@chromium.org on Wed, Mar 16, 2022, 10:21 PM EDT Project Member

Congratulations- the VRP Panel has decided to award you $5,000 for this report. A member of our finance team will be in touch soon to arrange payment. Thank you for this report and nice work!

Comment 34 by amyressler@chromium.org on Thu, Mar 17, 2022, 2:01 PM EDT Project Member

Labels: -Merge-Review-98 -Merge-Review-99

there are no further planned releases of M99 stable/M98 extended stable

Comment 35 by amyressler@google.com on Thu, Mar 17, 2022, 5:25 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 36 by maury...@gmail.com on Wed, Mar 23, 2022, 4:24 PM EDT

Appeal reward reason: Hi there,
I hope you're doing fine.

I'd like you to have a second look to the reward decision for this vulnerability as I think it was a little bit understimated.

Basically, it's a 1-click vulnerability which allows to:
- Leak the hashed credentials of Windows users.
- Relay the hashed credentials of Windows users to another server and, based on the user's privileges, read files from the target server or execute system commands (NTLM-relay).

TBH yesterday I saw this bug (https://bugs.chromium.org/p/chromium/issues/detail?id=1247389) which was rewarded

TBH yesterday I saw this bug (https://bugs.chromium.org/p/chromium/issues/detail?id=1247389) which was rewarded 10.000 $, so the double of mine, and I have the feeling this vulnerability is more severe than that one, that's why I tried to appeal the reward amount.

Thanks for your time.

Kind Regards,
smaury

Comment 37 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:42 PM EDT Project Member

Labels: Release-0-M100

Comment 38 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

Labels: CVE-2022-1128 CVE_description-missing

Comment 39 by amyressler@chromium.org on Wed, Mar 30, 2022, 7:57 PM EDT Project Member

Hello, the VRP Panel has reviewed this issue for reassessment and has decided the reward amount is appropriate for this report and this issue. The issue that you link in comparison does not leak hashes, but actual plaintext system and environment variables independent of the victim's user privileges. Thank you again for the report and reaching out with your request.

Comment 40 by maury...@gmail.com on Thu, Mar 31, 2022, 1:49 AM EDT

Thanks for the extra time spent on the reassessment.

Comment 41 by sheriffbot on Wed, Jun 15, 2022, 1:31 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

Comment 42 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

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

Labels: -CVE_description-missing --CVE_description-missing