☆ Starred by 1 user

Owner:	mek@chromium.org
CC:	asully@chromium.org mek@chromium.org brettw@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Storage>FileSystem UI>Browser>Downloads
Modified:	Apr 6, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-89
Target-87
Target-89
Merge-Rejected-87
Merge-Rejected-88
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
Release-0-M89
external_security_report
CVE-2021-21172

Issue 1150810: Security: File System Access API - getFileHandle() allowing to save .lnk files

Reported by macie...@gmail.com on Thu, Nov 19, 2020, 7:31 AM EST

Code

VULNERABILITY DETAILS
File System Access API - getFileHandle() allowing to save .lnk and .local files on windows.

Based on default/main chrome download function:
File System Access API - getFileHandle bypassing the function "IsShellIntegratedExtension":
https://source.chromium.org/chromium/chromium/src/+/master:net/base/filename_util_internal.cc;drc=1c58af32060fa0ef3cfd4037fdc7913092d16ba2;l=155?q=%20EnsureSafeExtension&ss=chromium

if extension ".lnk" or ".local" then Chrome should CHANGE extension to ".download", but not doing this:
https://source.chromium.org/chromium/chromium/src/+/master:net/base/filename_util_internal.cc;drc=1c58af32060fa0ef3cfd4037fdc7913092d16ba2;l=195?q=%20EnsureSafeExtension&ss=chromium

.lnk files are very dangerous and used in two ways:
1. Spoof extension on windows - totally hide the real extension of the file.
2. .lnk files may be used to execute arbitrary code (see https://nvd.nist.gov/vuln/detail/CVE-2010-2568).
https://www.thezdi.com/blog/2020/3/25/cve-2020-0729-remote-code-execution-through-lnk-files
Possible RCE by saving a .lnk file.

and

.local files may determine which DLLs to load for an application in Windows.

URL EXAMPLE: https://pulik.io/openandsave.html

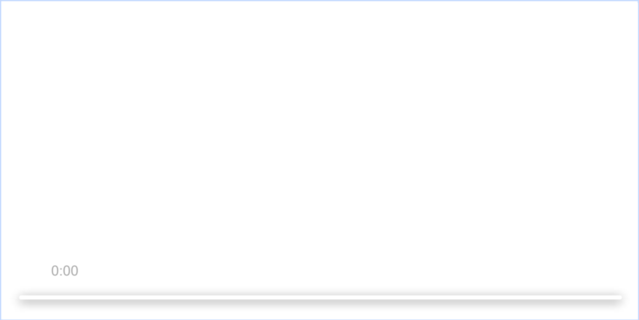
VERSION
Chrome Version: [87.0.4280.66] + [stable]
Operating System: [Windows 10 OS 10.0.18363 Build 18363]

REPRODUCTION CASE
1. Run openandsave.html or https://pulik.io/openandsave.html
2. Click "Select a folder where to create a new folder and image.jpg"
3. Choose a folder where files should be saved

SOLUTION
Replace ".lnk" and ".local" with ".download" or block downloading such a file.

Reporter credit: Maciej Pulikowski

lnkExample.mp4
18.7 MB Download



openandsave.html
1.8 KB View Download

picture20.png
38.5 KB View Download

picture21.png
24.0 KB View Download

Comment 1 by sheriffbot on Thu, Nov 19, 2020, 7:37 AM EST Project Member

Labels: reward-potential

Comment 2 by mbarb...@chromium.org on Thu, Nov 19, 2020, 2:22 PM EST Project Member

Owner: brettw@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable OS-Windows
Components: UI>Browser>Downloads

brettw: Would you mind taking a look at this or helping to find another owner?

Comment 3 by macie...@gmail.com on Thu, Nov 19, 2020, 2:27 PM EST

mek@chromium.org is the owner of similar issue I have found.

https://bugs.chromium.org/p/chromium/issues/detail?id=1140417

Comment 4 by sheriffbot on Sat, Nov 21, 2020, 1:03 PM EST Project Member

Labels: M-87 Target-87

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

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

Comment 5 by sheriffbot on Sat, Nov 21, 2020, 1:40 PM EST Project Member

Labels: -Pri-3 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 6 by sheriffbot on Sat, Nov 21, 2020, 2:35 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 7 by cthomp@chromium.org on Mon, Nov 30, 2020, 4:35 PM EST Project Member

Cc: mek@chromium.org asully@chromium.org
Components: Blink>Storage>FileSystem

Comment 8 by mek@chromium.org on Mon, Nov 30, 2020, 4:48 PM EST Project Member

Changing the extension to something like .download wouldn't really make sense for the File System Access API.

Also I'm not sure what is gained by blocking .local files. If a website can write to a .local file in a directory, it can also modify any executable in that same directory (both subject to safe browsing checks). So it doesn't seem like letting a website read/write .local files is any more dangerous than letting them read/write arbitrary other files in the same directory (not sure how .local files are used, there doesn't seem to be much information on the subject available that I can find).

Blocking access to .lnk files might be something worth considering, as that does seem at least somewhat more dangerous.

Comment 9 by macie...@gmail.com on Wed, Dec 2, 2020, 10:45 AM EST

@mek
Yes, you are right.
If we can edit/create files inside a folder then there are better ways to inject malware files.
For instance editing executables or DLL injection. So there is no need to block .local.

.lnk files can easily trick the user to run a PowerShell script, we can see it on the video.
In my opinion .lnk should be blocked :)

Comment 10 by mek@chromium.org on Wed, Dec 2, 2020, 2:15 PM EST Project Member

Status: Started (was: Assigned)
Owner: mek@chromium.org
Cc: brettw@chromium.org

Comment 11 by bugdroid on Wed, Dec 2, 2020, 6:55 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/004377929febd7cf7392932b01df7f4a0a362679

commit 004377929febd7cf7392932b01df7f4a0a362679
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Wed Dec 02 23:50:54 2020

[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.

This isn't directly using net::IsSafePortablePathComponent since what
is safe for the File System Access API is not the same as what is safe
for Downloads. As such currently this duplicates a lot of the
implementation of this method, but in a followup we should attempt to
unify these two implementations as much as possible.

~~Bug: 1150810~~, 1154757
Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Cr-Commit-Position: refs/heads/master@{#833042}

[modify] https://crrev.com/004377929febd7cf7392932b01df7f4a0a362679/content/browser/file_system_access/native_file_system_directory_handle_impl.cc
[modify] https://crrev.com/004377929febd7cf7392932b01df7f4a0a362679/content/browser/file_system_access/native_file_system_directory_handle_impl.h
[add] https://crrev.com/004377929febd7cf7392932b01df7f4a0a362679/content/browser/file_system_access/native_file_system_directory_handle_impl_unittest.cc
[modify] https://crrev.com/004377929febd7cf7392932b01df7f4a0a362679/content/test/BUILD.gn

Comment 12 by mek@chromium.org on Thu, Dec 3, 2020, 3:54 PM EST Project Member

Summary: Security: File System Access API - getFileHandle() allowing to save .lnk files (was: Security: File System Access API - getFileHandle() allowing to save .lnk and .local files)
Status: Fixed (was: Started)

With that CL it should no longer be possible to write to .lnk files using getFileHandle().

Should this be backported to M88? There is some risk of breakage of legit use cases since we're blocking a whole bunch of things that weren't previously blocked. On the other hand it seems like there would be enough M88 beta time left to catch issues before it reaches stable (and I don't expect issues).

Comment 13 by sheriffbot on Fri, Dec 4, 2020, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 14 by sheriffbot on Fri, Dec 4, 2020, 1:58 PM EST Project Member

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

Comment 15 by bugdroid on Fri, Dec 4, 2020, 3:10 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/455d1c44e8a3dc71984f19b0e7d85a2157b2862c

commit 455d1c44e8a3dc71984f19b0e7d85a2157b2862c
Author: Ben Pastene <bpastene@chromium.org>
Date: Fri Dec 04 20:04:37 2020

Revert "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle."

This reverts commit 004377929febd7cf7392932b01df7f4a0a362679.

Reason for revert: suspect to be causing apps.LaunchGallery failures on CrOS
https://bugs.chromium.org/p/chromium/issues/detail?id=1155028#c21

Original change's description:
> [FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.
>
> This isn't directly using net::IsSafePortablePathComponent since what
> is safe for the File System Access API is not the same as what is safe
> for Downloads. As such currently this duplicates a lot of the
> implementation of this method, but in a followup we should attempt to
> unify these two implementations as much as possible.
>
> ~~Bug: 1150810~~, 1154757
> Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
> Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> Reviewed-by: Victor Costan <pwnall@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#833042}

TBR=mek@chromium.org,pwnall@chromium.org,chromium-scoped@luci-project-accounts.iam.gserviceaccount.com

# Not skipping CQ checks because original CL landed > 1 day ago.

~~Bug: 1150810~~
Bug: 1154757
~~Bug: 1155028~~
Change-Id: I6c0fb2af7096d4f7f47d3e17a40c5a69105808cd
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2574931
Reviewed-by: Ben Pastene <bpastene@chromium.org>
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Ben Pastene <bpastene@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/heads/master@{#833820}

[modify] https://crrev.com/455d1c44e8a3dc71984f19b0e7d85a2157b2862c/content/browser/file_system_access/native_file_system_directory_handle_impl.cc
[modify] https://crrev.com/455d1c44e8a3dc71984f19b0e7d85a2157b2862c/content/browser/file_system_access/native_file_system_directory_handle_impl.h
[delete] https://crrev.com/3f2085ea3a5c46fa2a5eb0481a61b21a4b1a044c/content/browser/file_system_access/native_file_system_directory_handle_impl_unittest.cc
[modify] https://crrev.com/455d1c44e8a3dc71984f19b0e7d85a2157b2862c/content/test/BUILD.gn

Comment 16 by mek@chromium.org on Fri, Dec 4, 2020, 5:33 PM EST Project Member

Status: Started (was: Fixed)

Comment 17 by bugdroid on Sun, Dec 6, 2020, 11:23 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/2d41c3952d2851948a09ddcf3e97bae6c419b024

commit 2d41c3952d2851948a09ddcf3e97bae6c419b024

Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Mon Dec 07 04:22:13 2020

Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle."

This is a reland of 004377929febd7cf7392932b01df7f4a0a362679

The main difference is to make sure iterating over a directory doesn't
return files we don't want to expose either (and not CHECK failing if
such files are found when iterating).

Original change's description:
> [FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.
>
> This isn't directly using net::IsSafePortablePathComponent since what
> is safe for the File System Access API is not the same as what is safe
> for Downloads. As such currently this duplicates a lot of the
> implementation of this method, but in a followup we should attempt to
> unify these two implementations as much as possible.
>
> ~~Bug: 1150810~~, 1154757
> Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
> Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> Reviewed-by: Victor Costan <pwnall@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#833042}

~~Bug: 1150810~~
Bug: 1154757
Change-Id: I3341b9824a1ac4cbd6f100355960ad55b01f0753
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2575370
Commit-Queue: Victor Costan <pwnall@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Cr-Commit-Position: refs/heads/master@{#834118}

[modify] https://crrev.com/2d41c3952d2851948a09ddcf3e97bae6c419b024/content/browser/file_system_access/native_file_system_directory_handle_impl.cc
[modify] https://crrev.com/2d41c3952d2851948a09ddcf3e97bae6c419b024/content/browser/file_system_access/native_file_system_directory_handle_impl.h
[add] https://crrev.com/2d41c3952d2851948a09ddcf3e97bae6c419b024/content/browser/file_system_access/native_file_system_directory_handle_impl_unittest.cc
[modify] https://crrev.com/2d41c3952d2851948a09ddcf3e97bae6c419b024/content/browser/file_system_access/native_file_system_file_handle_impl_unittest.cc
[modify] https://crrev.com/2d41c3952d2851948a09ddcf3e97bae6c419b024/content/test/BUILD.gn

Comment 18 by bugdroid on Mon, Dec 7, 2020, 1:09 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/f28329389fc82380b18c4e89ce276d1ef0b47f48

commit f28329389fc82380b18c4e89ce276d1ef0b47f48
Author: Alexey Baskakov <loyso@chromium.org>
Date: Mon Dec 07 06:06:53 2020

Revert "Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.""

This reverts commit 2d41c3952d2851948a09ddcf3e97bae6c419b024.

Reason for revert: Failed tests on Wim7 builder
https://ci.chromium.org/ui/p/chromium/builders/ci/Win7%20Tests%20(1)/111291/overview

Original change's description:
> Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle."
>
> This is a reland of 004377929febd7cf7392932b01df7f4a0a362679
>
> The main difference is to make sure iterating over a directory doesn't
> return files we don't want to expose either (and not CHECK failing if
> such files are found when iterating).
>
> Original change's description:
> > [FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.
> >
> > This isn't directly using net::IsSafePortablePathComponent since what
> > is safe for the File System Access API is not the same as what is safe
> > for Downloads. As such currently this duplicates a lot of the
> > implementation of this method, but in a followup we should attempt to
> > unify these two implementations as much as possible.
> >
> > ~~Bug: 1150810~~, 1154757
> > Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
> > Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> > Reviewed-by: Victor Costan <pwnall@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#833042}
>
> ~~Bug: 1150810~~
> Bug: 1154757
> Change-Id: I3341b9824a1ac4cbd6f100355960ad55b01f0753
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2575370
> Commit-Queue: Victor Costan <pwnall@chromium.org>
> Reviewed-by: Victor Costan <pwnall@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#834118}

TBR=mek@chromium.org,pwnall@chromium.org,chromium-scoped@luci-project-accounts.iam.gserviceaccount.com

Change-Id: I4cf610510109c47f62c59921fbe95a78b098a1a5
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
~~Bug: 1150810~~
Bug: 1154757
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2576223
Reviewed-by: Alexey Baskakov <loyso@chromium.org>
Commit-Queue: Alexey Baskakov <loyso@chromium.org>
Cr-Commit-Position: refs/heads/master@{#834133}

[modify] https://crrev.com/f28329389fc82380b18c4e89ce276d1ef0b47f48/content/browser/file_system_access/native_file_system_directory_handle_impl.cc

[modify] https://crrev.com/f28329389fc82380b18c4e89ce276d1ef0b47f48/content/browser/file_system_access/native_file_system_directory_handle_impl.h
[delete] https://crrev.com/61484e7ce2dba646bf93445c30ea2b1da68887c4/content/browser/file_system_access/native_file_system_directory_handle_impl_unittest.cc
[modify] https://crrev.com/f28329389fc82380b18c4e89ce276d1ef0b47f48/content/browser/file_system_access/native_file_system_file_handle_impl_unittest.cc
[modify] https://crrev.com/f28329389fc82380b18c4e89ce276d1ef0b47f48/content/test/BUILD.gn

Comment 19 by bugdroid on Tue, Dec 8, 2020, 2:21 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a66dbdcf64938c63674aec4dea09ffcb918e456b

commit a66dbdcf64938c63674aec4dea09ffcb918e456b
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Tue Dec 08 07:20:47 2020

Reland "Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.""

This is a reland of 2d41c3952d2851948a09ddcf3e97bae6c419b024

The added test was modified to no longer assert that all unsafe files
were written to disk successfully. This should make the test pass (albeit
with less stringent checks) on file systems/platforms that don't allow
all unsafe file names.

Original change's description:
> Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle."
>
> This is a reland of 004377929febd7cf7392932b01df7f4a0a362679
>
> The main difference is to make sure iterating over a directory doesn't
> return files we don't want to expose either (and not CHECK failing if
> such files are found when iterating).
>
> Original change's description:
> > [FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.
> >
> > This isn't directly using net::IsSafePortablePathComponent since what
> > is safe for the File System Access API is not the same as what is safe
> > for Downloads. As such currently this duplicates a lot of the
> > implementation of this method, but in a followup we should attempt to
> > unify these two implementations as much as possible.
> >
> > ~~Bug: 1150810~~, 1154757
> > Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
> > Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> > Reviewed-by: Victor Costan <pwnall@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#833042}
>
> ~~Bug: 1150810~~
> Bug: 1154757
> Change-Id: I3341b9824a1ac4cbd6f100355960ad55b01f0753
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2575370
> Commit-Queue: Victor Costan <pwnall@chromium.org>
> Reviewed-by: Victor Costan <pwnall@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#834118}

~~Bug: 1150810~~
Bug: 1154757
Change-Id: Ie5cad9a7b2383c89b96e8a7be6cfe75ad2555fa6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2577614
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Cr-Commit-Position: refs/heads/master@{#834598}

[modify] https://crrev.com/a66dbdcf64938c63674aec4dea09ffcb918e456b/content/test/BUILD.gn
[modify] https://crrev.com/a66dbdcf64938c63674aec4dea09ffcb918e456b/content/browser/file_system_access/native_file_system_file_handle_impl_unittest.cc
[modify] https://crrev.com/a66dbdcf64938c63674aec4dea09ffcb918e456b/content/browser/file_system_access/native_file_system_directory_handle_impl.cc
[modify] https://crrev.com/a66dbdcf64938c63674aec4dea09ffcb918e456b/content/browser/file_system_access/native_file_system_directory_handle_impl.h
[add] https://crrev.com/a66dbdcf64938c63674aec4dea09ffcb918e456b/content/browser/file_system_access/native_file_system_directory_handle_impl_unittest.cc

Comment 20 by mek@chromium.org on Wed, Dec 9, 2020, 6:28 PM EST Project Member

Status: Fixed (was: Started)

Comment 21 by sheriffbot on Sat, Dec 12, 2020, 2:22 PM EST Project Member

Labels: Merge-Request-88

Requesting merge to beta M88 because latest trunk commit (833042) appears to be after beta branch point (827102).

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

Comment 22 by sheriffbot on Sat, Dec 12, 2020, 2:25 PM EST Project Member

Labels: -Merge-Request-88 Merge-Review-88 Hotlist-Merge-Review

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: govind@(Android), bindusuvarna@(iOS), dgagnon@(ChromeOS), srinivassista @(Desktop)

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

Comment 23 by srinivassista@google.com on Sat, Dec 12, 2020, 6:46 PM EST Project Member

pls answer comment #22 for merge review

Comment 24 by srinivassista@google.com on Tue, Dec 15, 2020, 1:19 PM EST Project Member

friendly ping ^

Comment 25 by adetaylor@google.com on Tue, Dec 15, 2020, 2:01 PM EST Project Member

Labels: -Merge-Review-88 Merge-Rejected-88 Merge-Rejected-87

I think #c12 probably covers most of the information we need regarding stability risk.

Given the concerns expressed in that comment, plus the reverts/relands, and the fact that this is medium severity, I'm not going to merge this either to M88 or M87 but instead wait for it to organically be released in M89.

Comment 26 by adetaylor@google.com on Wed, Dec 16, 2020, 7:08 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 adetaylor@google.com on Wed, Dec 16, 2020, 7:22 PM EST Project Member

Congratulations, the VRP panel has decided to award $1000 for this bug.

Comment 28 by adetaylor@google.com on Thu, Dec 17, 2020, 1:36 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 29 by adetaylor@google.com on Wed, Jan 20, 2021, 6:57 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 30 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 31 by adetaylor@google.com on Mon, Mar 1, 2021, 7:27 PM EST Project Member

Labels: CVE-2021-21172 CVE_description-missing

Comment 32 by vsavu@google.com on Wed, Mar 3, 2021, 5:52 AM EST Project Member

Labels: a11y-audit-2020 LTS-Merge-Request-86

Comment 33 by vsavu@google.com on Wed, Mar 3, 2021, 5:52 AM EST Project Member

Labels: -a11y-audit-2020

Comment 34 by vsavu@google.com on Wed, Mar 3, 2021, 6:01 AM EST Project Member

Labels: LTS-Security-86

Comment 35 by gianluca@google.com on Wed, Mar 3, 2021, 10:37 AM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 36 by sheriffbot on Wed, Mar 3, 2021, 12:22 PM EST Project Member

Labels: -M-87 Target-89 M-89

Comment 37 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 38 by sheriffbot on Thu, Mar 18, 2021, 1:50 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 39 by Git Watcher on Thu, Apr 1, 2021, 4:28 AM EDT Project Member

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5fea89416a4df55bc84983c5bf3a9b9105d377d1

commit 5fea89416a4df55bc84983c5bf3a9b9105d377d1
Author: Victor-Gabriel Savu <vsavu@google.com>
Date: Thu Apr 01 08:27:33 2021

Reland "Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.""

This is a reland of 2d41c3952d2851948a09ddcf3e97bae6c419b024

The added test was modified to no longer assert that all unsafe files
were written to disk successfully. This should make the test pass (albeit
with less stringent checks) on file systems/platforms that don't allow
all unsafe file names.

[M86-Merge]: Changes applied to moved files.
Chanved to include bind_test_util.h.
Updated unit tests to use the old API.

Original change's description:
> Reland "[FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle."

>
> This is a reland of 004377929febd7cf7392932b01df7f4a0a362679
>
> The main difference is to make sure iterating over a directory doesn't
> return files we don't want to expose either (and not CHECK failing if
> such files are found when iterating).
>
> Original change's description:
> > [FSA] Add IsSafePathComponent checks to GetFile/GetDirectoryHandle.
> >
> > This isn't directly using net::IsSafePortablePathComponent since what
> > is safe for the File System Access API is not the same as what is safe
> > for Downloads. As such currently this duplicates a lot of the
> > implementation of this method, but in a followup we should attempt to
> > unify these two implementations as much as possible.
> >
> > ~~Bug: 1150810~~, 1154757
> > Change-Id: Iba4c92ef5f1cd924aa22b9dd201762d48b4bbc3b
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2568383
> > Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> > Reviewed-by: Victor Costan <pwnall@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#833042}
>
> ~~Bug: 1150810~~
> Bug: 1154757
> Change-Id: I3341b9824a1ac4cbd6f100355960ad55b01f0753
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2575370
> Commit-Queue: Victor Costan <pwnall@chromium.org>
> Reviewed-by: Victor Costan <pwnall@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#834118}

(cherry picked from commit a66dbdcf64938c63674aec4dea09ffcb918e456b)

~~Bug: 1150810~~
Bug: 1154757
Change-Id: Ie5cad9a7b2383c89b96e8a7be6cfe75ad2555fa6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2577614
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#834598}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2731652
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1589}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/5fea89416a4df55bc84983c5bf3a9b9105d377d1/content/browser/native_file_system/native_file_system_directory_handle_impl.cc
[modify] https://crrev.com/5fea89416a4df55bc84983c5bf3a9b9105d377d1/content/browser/native_file_system/native_file_system_directory_handle_impl.h
[add] https://crrev.com/5fea89416a4df55bc84983c5bf3a9b9105d377d1/content/browser/native_file_system/native_file_system_directory_handle_impl_unittest.cc
[modify] https://crrev.com/5fea89416a4df55bc84983c5bf3a9b9105d377d1/content/browser/native_file_system/native_file_system_file_handle_impl_unittest.cc
[modify] https://crrev.com/5fea89416a4df55bc84983c5bf3a9b9105d377d1/content/test/BUILD.gn

Comment 40 by vsavu@google.com on Tue, Apr 6, 2021, 10:32 AM EDT Project Member

Labels: -LTS-Merge-Approved-86 -LTS-Merge-Request-86 LTR-Merged-86