Starred by 5 users

Owner:	qin...@chromium.org
CC:	nyquist@chromium.org dcheng@chromium.org amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Downloads
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Android
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Reward-1000
Security_Severity-Medium
Hotlist-Merge-Approved
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-100
FoundIn-93
Security_Impact-Extended
Release-0-M101
CVE-2022-1495

Issue 1301180: Security: Bypass Apk Warning In Andriod

Reported by pufin...@gmail.com on Sun, Feb 27, 2022, 2:59 PM EST

Code

Peace Be Upon You

Bypass Apk Warning In Chrome Andriod
Using A Basic Html/Js Code
Please Check The Code

VERSION
Chrome Version: [93.0.4577.82]
Operating System: [Andriod]

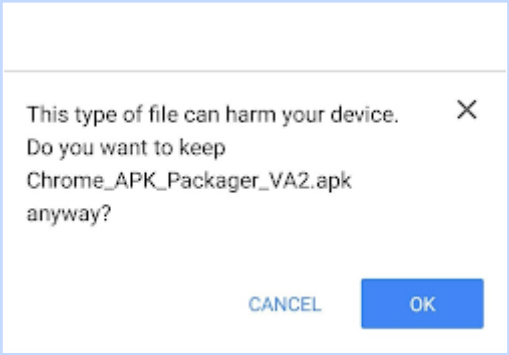
if you have any questions let me know

Thank You

Puf Demo.html
1.1 KB View Download

Comment 1 by pufin...@gmail.com on Sun, Feb 27, 2022, 3:01 PM EST

Apk Warning.jpg
77.5 KB View Download



Comment 2 by sheriffbot on Sun, Feb 27, 2022, 3:02 PM EST

Labels: external_security_report

Comment 3 by pufin...@gmail.com on Tue, Mar 1, 2022, 1:32 AM EST

Any Update ?

Comment 4 by dcheng@chromium.org on Wed, Mar 2, 2022, 8:39 PM EST

Labels: Needs-Feedback

I tried this out on an Android device. I navigated to the test page and clicked [Open]. I got a dialog about where to save the file, followed immediately afterwards by a dialog that APKs might be harmful. So I don't see a bypass.

Can you clarify the steps, or explain where the bypass is?

Comment 5 Deleted

Comment 6 by sheriffbot on Thu, Mar 3, 2022, 9:25 AM EST

Cc: dcheng@chromium.org
Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 7 by pufin...@gmail.com on Thu, Mar 3, 2022, 9:26 AM EST

Peace Be Upon You

I Have Tested In my Andriod

it's working here

please check this file

thank you.

Puf 2.html
742 bytes View Download

Comment 8 by dcheng@chromium.org on Fri, Mar 4, 2022, 3:03 AM EST

Status: Assigned (was: Unconfirmed)
Owner: qin...@chromium.org
Labels: FoundIn-93 Security_Severity-Medium OS-Android Pri-1
Components: UI>Browser>Downloads

Simplified repro:

```
<script>
function Puf(uri, name) {
  var link = document.createElement("a");
  link.download = name;
  link.href = uri;
  link.click();
}
function openWin()
{
Puf("data:application/vnd.android.package-archive;base64,UGVhY2UgQmUgVXBvbiBZb3U=", "apk.puf")
}
</script>
<input type="button" onclick="openWin();" value="open"/>
```

The problem is that the download is called apk.puf, and doesn't trigger the dangerous download prompt, but when we actually save the file, we add the apk extension (probably because of the MIME type).

Tagging with FoundIn-93 based on reporter's Chrome version, though the oldest I was able to test was 99.

Comment 9 by sheriffbot on Fri, Mar 4, 2022, 3:05 AM EST

Labels: Security_Impact-Extended

Comment 10 by pufin...@gmail.com on Fri, Mar 4, 2022, 4:02 AM EST

Peace Be Upon You

Is this valid bug sir ?

Thank you

Comment 11 by sheriffbot on Fri, Mar 4, 2022, 12:52 PM EST

Labels: M-100 Target-100

Setting milestone and target because of medium severity.

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

Comment 12 by dcheng@chromium.org on Sat, Mar 5, 2022, 2:18 AM EST

Yes, it looks like a valid bug to me--that's why it's tagged with a severity and an impact.

Comment 13 by pufin...@gmail.com on Sat, Mar 5, 2022, 7:19 AM EST

Thank You ~

Comment 14 by qin...@chromium.org on Mon, Mar 7, 2022, 11:43 AM EST

This is an interesting bug. Chrome will create the filename apk.puf for the download. However, Android uses MediaStore to store all the downloads since Q. And MediaStore will change the file name when chrome creates the content URI.

Comment 15 by qin...@chromium.org on Wed, Mar 9, 2022, 2:33 PM EST

Cc: xingliu@chromium.org

Comment 16 by qin...@chromium.org on Wed, Mar 9, 2022, 5:09 PM EST

Cc: nyquist@chromium.org

Comment 17 by pufin...@gmail.com on Thu, Mar 10, 2022, 6:37 AM EST

Peace Be Upon You

Are there any updates sir?

Thank you

Comment 18 by Git Watcher on Thu, Mar 17, 2022, 5:12 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/49bbefe192eabd120f9af9aa1e18ab0116cce891

commit 49bbefe192eabd120f9af9aa1e18ab0116cce891

Author: Min Qin <qinmin@chromium.org>
Date: Thu Mar 17 21:11:18 2022

Fix an issue dangerous dialog is not shown for some apk download

On Android Q+, download will create a different intermediate content Uri after target determination. However, creating the content Uri might cause the file name to change, as Android tries to correct the file name using MIME type. And the new file name may be of a dangerous type.
However, the dangerous file check happens in target determination. So creating the intermediate content Uri later allows such file names to bypass dangerous file check.
This CL fixes the issue by moving content URI creation into target determination stage, right before dangerous download check. And this will also simplify the logic in DownloadItemImpl as it now gets the target content Uri instead of an unused file path after target determination.

~~BUG=1301180~~

Change-Id: Ie4561e8d0b4b3a87ec7a041f3ac71f23866fce04
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508375
Reviewed-by: Xing Liu <xingliu@chromium.org>
Reviewed-by: Alex Moshchuk <alexmos@chromium.org>
Reviewed-by: Junbo Ke <juke@chromium.org>
Reviewed-by: Clark DuVall <cduvall@chromium.org>
Reviewed-by: Tommy Nyquist <nyquist@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Commit-Position: refs/heads/main@{#982422}

[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/download_file.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/download_target_determiner_unittest.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/chrome_download_manager_delegate.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/download_target_info.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/in_progress_download_manager.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/weblayer/browser/download_manager_delegate_impl.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/download_target_determiner.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/content/shell/browser/shell_download_manager_delegate.cc
[modify]

https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/content/public/browser/download_manager_delegate.h
[modify]

https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chromecast/browser/cast_download_manager_delegate.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/download_utils.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/content/browser/download/download_manager_impl.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/download_item_impl_delegate.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/download_item_impl_unittest.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/lifetime/browser_close_manager_browsertest.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/download_item_impl.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/download_target_determiner_delegate.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/download_target_determiner.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/chrome_download_manager_delegate.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/content/browser/download/download_manager_impl_unittest.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/download_file_impl.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/download_utils.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/chrome/browser/download/chrome_download_manager_delegate_unittest.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/download_item_impl_delegate.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/internal/common/download_file_impl.cc
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/mock_download_item_impl.h
[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/content/browser/devtools/protocol/devtools_download_manager_delegate.cc

[modify]
https://crrev.com/49bbefe192eabd120f9af9aa1e18ab0116cce891/components/download/public/common/download_item_impl.h

mpi.n

Comment 19 by Git Watcher on Fri, Mar 18, 2022, 3:09 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5bfe30827bd88638cfc6438ec4a283463e55bbb1

commit 5bfe30827bd88638cfc6438ec4a283463e55bbb1
Author: Min Qin <qinmin@chromium.org>
Date: Fri Mar 18 07:08:45 2022

Fix test failure on android 11 bots

~~BUG=1301180~~

Change-Id: I78789baf21e253df9705c8b433da8c088689e127
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3534549
Reviewed-by: Shakti Sahu <shaktisahu@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Commit-Position: refs/heads/main@{#982606}

[modify]
https://crrev.com/5bfe30827bd88638cfc6438ec4a283463e55bbb1/components/download/internal/common/download_item_impl_unittest.cc
[modify]
https://crrev.com/5bfe30827bd88638cfc6438ec4a283463e55bbb1/chrome/browser/download/chrome_download_manager_delegate_unittest.cc

Comment 20 by mattm@chromium.org on Fri, Mar 18, 2022, 2:39 PM EDT

~~Issue 1307647~~ has been merged into this issue.

Comment 21 by pufin...@gmail.com on Wed, Mar 23, 2022, 6:25 AM EDT

Peace Be Upon You

Are there any updates sir?

Thank you

Comment 22 by sheriffbot on Thu, Mar 24, 2022, 12:21 PM EDT

qinmin: 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?

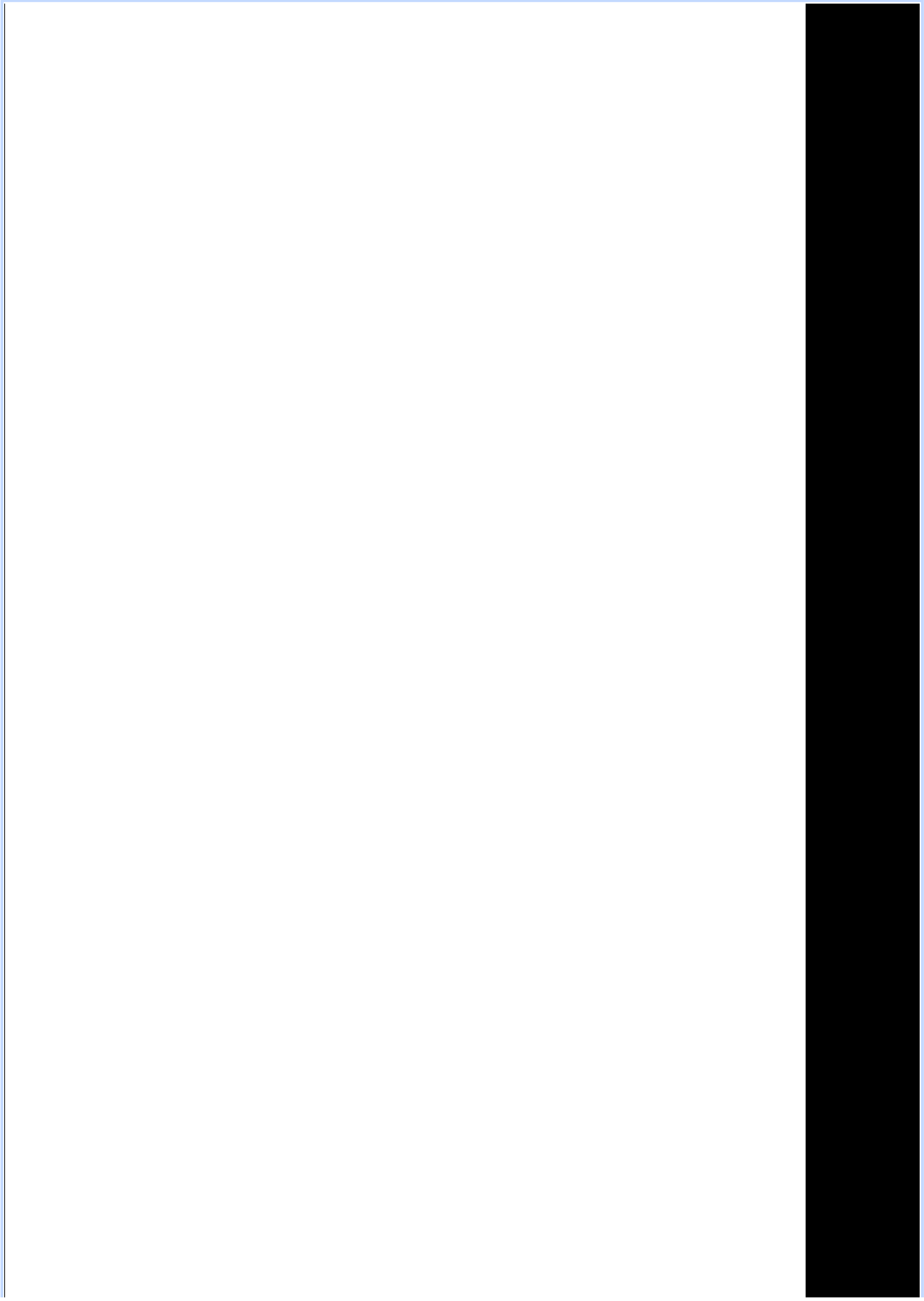
If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

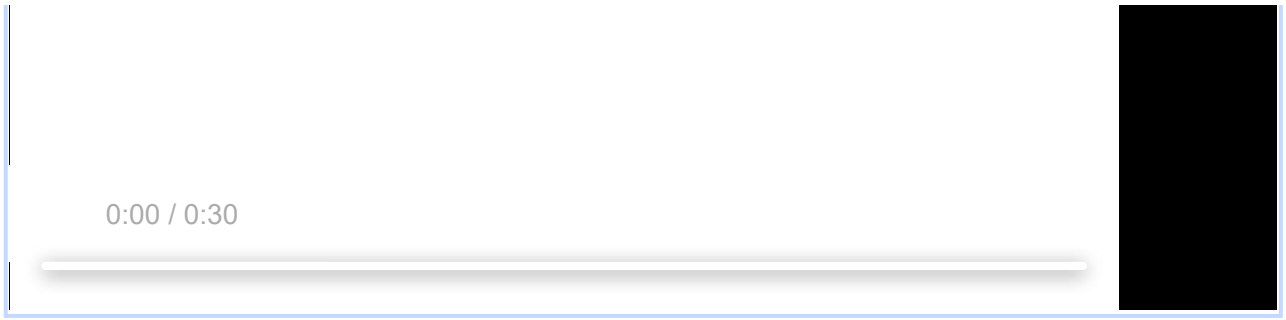
Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 23 by pufin...@gmail.com on Fri, Mar 25, 2022, 12:04 AM EDT

puf2.mp4
421 KB View Download





Comment 24 by pufin...@gmail.com on Mon, Mar 28, 2022, 2:05 PM EDT

Peace Be Upon You

- is this eligible for VRP?

Thank You

Comment 25 by qin...@chromium.org on Mon, Mar 28, 2022, 2:16 PM EDT

I guess yes, but will leave it to the security team to decide.

Comment 26 by qin...@chromium.org on Mon, Mar 28, 2022, 2:16 PM EDT

Status: Fixed (was: Assigned)

Comment 27 by pufin...@gmail.com on Mon, Mar 28, 2022, 2:17 PM EDT

Thank You Very Much Sir

Comment 28 by pufin...@gmail.com on Tue, Mar 29, 2022, 4:03 AM EDT

Peace Be Upon You

Any update regarding reward ?

Please Let me Know

Thank You

Comment 29 by sheriffbot on Tue, Mar 29, 2022, 12:41 PM EDT

Labels: reward-topanel

Comment 30 by sheriffbot on Tue, Mar 29, 2022, 1:40 PM EDT

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

Comment 31 by sheriffbot on Tue, Mar 29, 2022, 2:11 PM EDT

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

Requesting merge to beta M100 because latest trunk commit (982606) appears to be after beta branch point (972766).

Requesting merge to dev M101 because latest trunk commit (982606) appears to be after dev branch point (982481).

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

Comment 32 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT

Labels: -Merge-Request-101 Hotlist-Merge-Approved Merge-Approved-101

Merge approved: your change passed merge requirements and is auto-approved for M101. Please go ahead and merge the CL to branch 4951 (refs/branch-heads/4951) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 33 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT

Labels: -Merge-Request-100 Hotlist-Merge-Review 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 34 by amyressler@chromium.org on Thu, Mar 31, 2022, 3:46 PM EDT

Cc: amyressler@chromium.org
Labels: -Merge-Review-100

Hi qinmin@ -- this issue is already approved for merge to M101 (branch 4951), please merge this fix at your earliest convenience.

As this is a rather textually large and non-trivial for a medium severity issue and M100 is now Stable channel, I am believe it may be best to hold off merging this to Stable channel for a respin and waiting to get this into M101. Please let me know if you see any issues with that.

Comment 35 by amyressler@chromium.org on Thu, Mar 31, 2022, 3:48 PM EDT

in response to comment #24 -- hello and thanks to your question, now that this issue has been resolved it will sent to the VRP Panel for consideration for a potential reward. This did not make the cutoff for this week, so it may be a couple of week until this issue is evaluated. The reward decision will be applied directly to this report, so you will see an update here when that happens.

Comment 36 by pufin...@gmail.com on Thu, Mar 31, 2022, 8:33 PM EDT

Thank You So Much Sir

i have one question Sir
My English is Not Good, it will effect My reward ?
Thank You

Comment 37 by amyressler@chromium.org on Fri, Apr 1, 2022, 10:33 AM EDT

Hello, thanks for your question, but no -- your English proficiency does not impact the VRP Reward. Reward judgements are solely made based on:
- bug impact
- report quality (how well the report explains the issue and impact of it and how well it demonstrates potential exploitability)
- potential bonuses for exploits and analysis

Please see https://g.co/chrome/vrp for our full VRP rules and policies.

Comment 38 Deleted

Comment 39 by pufin...@gmail.com on Fri, Apr 1, 2022, 10:40 AM EDT

Thank You very Much Sir

For guiding me

i'm not good in english & My explanation is also not good

i'm trying my best to explain in a better way That's why i always try to make POC videos

Because of explanation i'm afraid it will effect vrp reward rules

thanks once again sir

Comment 40 by sheriffbot on Tue, Apr 5, 2022, 12:21 PM EDT

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 41 by qin...@chromium.org on Tue, Apr 5, 2022, 12:48 PM EDT

Labels: -Merge-Approved-101

Comment 42 by xingliu@chromium.org on Tue, Apr 5, 2022, 12:50 PM EDT

Cc: -xingliu@chromium.org

Comment 43 by amyressler@google.com on Wed, Apr 13, 2022, 7:42 PM EDT

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

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 44 by amyressler@chromium.org on Wed, Apr 13, 2022, 8:12 PM EDT

Congratulations! The VRP Panel has decided to award you $1,000 for your report. A member of our finance team will be in touch with you soon to arrange payment.
Please let us know the name (or tag/handle/other identifier) you would like us to use in providing acknowledgement to you for reporting this issue.
Thank you for your efforts and reporting this issue to us.

Comment 45 by pufin...@gmail.com on Fri, Apr 15, 2022, 2:55 AM EDT

Thank You! Sir

Name : Umar Farooq

Comment 46 by amyressler@google.com on Fri, Apr 15, 2022, 10:01 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 47 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:10 PM EDT

Labels: Release-0-M101

Comment 48 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT

Labels: CVE-2022-1495 CVE_description-missing

Comment 49 by sheriffbot on Tue, Jul 5, 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 50 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 51 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing