Starred by 2 users

Owner: lucmult@chromium.org

CC: matthewjoseph@google.com
rzanoni@google.com
pmonette@chromium.org
lucmult@chromium.org
zentaro@chromium.org
hardi...@google.com
majewski@chromium.org
dcheng@chromium.org
gavinwill@chromium.org

Status: Fixed *(Closed)*

Components: Internals>Printing
Platform>Apps>FileManager

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Chrome

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-98
FoundIn-99
FoundIn-100
M-101
Target-101
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4951
merge-merged-101

Release-0-M101
CVE-2022-1496

Issue 1306391: Security: Use-After-Free in SelectFileDialog

Reported by vulb...@gmail.com on Tue, Mar 15, 2022, 3:55 AM EDT

Code

VULNERABILITY DETAILS

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.cc;l=321;drc=35a6eae48ee9838a2672b9a1ef7b149d3f7983b2;bpv=1;bpt=1

```
  web_ui()->RegisterMessageCallback(
      "selectPPDFile",
      base::BindRepeating(&CupsPrintersHandler::HandleSelectPPDFile,//<--
                          base::Unretained(this)));
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.cc;l=887;drc=35a6eae48ee9838a2672b9a1ef7b149d3f7983b2;bpv=1;bpt=1

```
void CupsPrintersHandler::HandleSelectPPDFile(const base::Value::List& args) {
  CHECK_EQ(1U, args.size());
  webui_callback_id_ = args[0].GetString();

  base::FilePath downloads_path =
      DownloadPrefs::FromDownloadManager(profile_->GetDownloadManager())
          ->DownloadPath();

  content::WebContents* web_contents = web_ui()->GetWebContents();
  select_file_dialog_ = ui::SelectFileDialog::Create(
      this, std::make_unique<ChromeSelectFilePolicy>(web_contents));

  gfx::NativeWindow owning_window =
      web_contents ? chrome::FindBrowserWithWebContents(web_contents)
                         ->window()
                         ->GetNativeWindow()
                   : gfx::kNullNativeWindow;

  ui::SelectFileDialog::FileTypeInfo file_type_info;
  file_type_info.extensions.push_back({"ppd"});
  file_type_info.extensions.push_back({"ppd.gz"});
  select_file_dialog_->SelectFile(
      ui::SelectFileDialog::SELECT_OPEN_FILE, std::u16string(), downloads_path,
      &file_type_info, 0, FILE_PATH_LITERAL(""), owning_window, nullptr);
}


CupsPrintersHandler::~CupsPrintersHandler() = default;
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=565;drc=35a6eae48ee9838a2672b9a1ef7b149d3f7983b2;

```
void SelectFileDialogExtension::NotifyListener() {
  if (!listener_)
```

```
    return;

  // The selected files are passed by reference to the listener. Ensure they
  // outlive the dialog if it is immediately deleted by the listener.
  std::vector<ui::SelectedFileInfo> selection_files =
      std::move(selection_files_);
  selection_files_.clear();

  switch (selection_type_) {
    case CANCEL:
      listener_->FileSelectionCanceled(params_);
      break;
    case SINGLE_FILE:
      listener_->FileSelectedWithExtraInfo(selection_files[0], selection_index_,
                                           params_);
      break;
    case MULTIPLE_FILES:
      listener_->MultiFilesSelectedWithExtraInfo(selection_files, params_);
      break;
    default:
      NOTREACHED();
      break;
  }
}
```

Like ~~crbug.com/1201032~~, If call `CupsPrintersHandler::HandleSelectPPDFile` two times in succession, free `CupsPrintersHandler` and select a folder or close with the SelectFileDialog, UAF is triggered in `SelectFileDialogExtension::NotifyListener`.

VERSION
Chrome Version:
Operating System: chromeos

REPRODUCTION CASE
1. navigate to "chrome://diagnostics"
2. open debug console with F12
3. copy & paste & run following script

```
function sleep(delay) {
  return new Promise((resolve) => setTimeout(resolve, delay));
}

var tab1 = open("chrome://os-settings/cupsPrinters");
await sleep(3000);

with(tab1) {
  chrome.send("selectPPDFile",["12"]);
  chrome.send("selectPPDFile",["12"]);
```

```
}
await sleep(3000)
tab1.close();
```
4. after tab1 is closed, choose a folder or close the SelectFileDialog

asan_with_sym.log
21.6 KB View Download

Comment 1 by vulb...@gmail.com on Tue, Mar 15, 2022, 3:58 AM EDT

sorry ,copy wrong for the REPRODUCTION CASE

REPRODUCTION CASE
1. navigate to "chrome://os-settings/cupsPrinters"
2. open debug console with F12
3. copy & paste & run following script
```
function sleep(delay) {
  return new Promise((resolve) => setTimeout(resolve, delay));
}

var tab1 = open("chrome://os-settings/cupsPrinters");
await sleep(3000);

with(tab1) {
  chrome.send("selectPPDFile",["12"]);
  chrome.send("selectPPDFile",["12"]);
}
await sleep(3000)
tab1.close();
```
4. after tab1 is closed, choose a folder or close the SelectFileDialog

Comment 2 by sheriffbot on Tue, Mar 15, 2022, 4:01 AM EDT

Labels: external_security_report

Comment 3 by vulb...@gmail.com on Tue, Mar 15, 2022, 4:20 AM EDT

hello,Here is another bug, `scanning_handler` is similar to this.

https://source.chromium.org/chromium/chromium/src/+/main:ash/webui/scanning/scanning_handler.cc;l=51;drc=35a6eae48ee9838a2672b9a1ef7b149d3f7983b2;bpv=1;bpt=1
```
  web_ui()->RegisterDeprecatedMessageCallback(
      "requestScanToLocation",
      base::BindRepeating(&ScanningHandler::HandleRequestScanToLocation,    //<--
                          base::Unretained(this)));
```

https://source.chromium.org/chromium/chromium/src/+/main:ash/webui/scanning/scanning_handler.cc;l=157;drc=35a6eae4

8ee9838a2672b9a1ef7b149d3f7983b2

```
void ScanningHandler::HandleRequestScanToLocation(const base::ListValue* args) {
  CHECK_EQ(1U, args->GetListDeprecated().size());
  scan_location_callback_id_ = args->GetListDeprecated()[0].GetString();

  content::WebContents* web_contents = web_ui()->GetWebContents();
  gfx::NativeWindow owning_window =
      web_contents ? web_contents->GetTopLevelNativeWindow()
                   : gfx::kNullNativeWindow;
  select_file_dialog_ = ui::SelectFileDialog::Create(                    //<--
      this, scanning_app_delegate_->CreateChromeSelectFilePolicy());
  select_file_dialog_->SelectFile(
      ui::SelectFileDialog::SELECT_FOLDER,
      l10n_util::GetStringUTF16(IDS_SCANNING_APP_SELECT_DIALOG_TITLE),
      base::FilePath() /* default_path */, nullptr /* file_types */,
      0 /* file_type_index */,
      base::FilePath::StringType() /* default_extension */, owning_window,
      nullptr /* params */);
}



ScanningHandler::~ScanningHandler() = default;
```

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=565;drc=35a6eae48ee9838a2672b9a1ef7b149d3f7983b2;

```
void SelectFileDialogExtension::NotifyListener() {
  if (!listener_)
    return;

  // The selected files are passed by reference to the listener. Ensure they
  // outlive the dialog if it is immediately deleted by the listener.
  std::vector<ui::SelectedFileInfo> selection_files =
      std::move(selection_files_);
  selection_files_.clear();

  switch (selection_type_) {
    case CANCEL:
      listener_->FileSelectionCanceled(params_);
      break;
    case SINGLE_FILE:
      listener_->FileSelectedWithExtraInfo(selection_files[0], selection_index_,
                                           params_);
      break;
    case MULTIPLE_FILES:
      listener_->MultiFilesSelectedWithExtraInfo(selection_files, params_);
      break;
    default:
      NOTREACHED();
      break;
  }
}
```

Comment 4 by mattm@chromium.org on Thu, Mar 17, 2022, 6:55 PM EDT

Labels: OS-Chrome

Comment 5 by hardi...@google.com on Mon, Mar 21, 2022, 1:00 PM EDT

Components: Internals>Printing

Comment 6 by hardi...@google.com on Mon, Mar 21, 2022, 1:25 PM EDT

Labels: Security_Severity-Medium Pri-2
Components: Platform>Apps>FileManager

Comment 7 by thestig@chromium.org on Mon, Mar 21, 2022, 1:26 PM EDT

Cc: gavinwill@chromium.org dcheng@chromium.org

This may overlap with ~~bug 1305068~~ and ~~bug 1304145~~.

Comment 8 by hardi...@google.com on Mon, Mar 21, 2022, 1:26 PM EDT

Owner: majewski@chromium.org

Assigning to an owner:

majewski@ could you please look into it?

Comment 9 by hardi...@google.com on Mon, Mar 21, 2022, 1:26 PM EDT

Cc: hardi...@google.com

Comment 10 by sheriffbot on Mon, Mar 21, 2022, 2:27 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 11 by gavinwill@chromium.org on Mon, Mar 21, 2022, 3:09 PM EDT

Owner: gavinwill@chromium.org

Comment 12 by hardi...@google.com on Tue, Mar 22, 2022, 12:40 PM EDT

Cc: majewski@chromium.org

Comment 13 by sheriffbot on Tue, Mar 22, 2022, 1:18 PM EDT

Labels: -Pri-2 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 14 by majewski@chromium.org on Tue, Mar 22, 2022, 11:08 PM EDT

hardikgoyal@ could you please be a bit more specific and verbose? What am I looking specifically for? Confirm that the bug affects SelectFileDialog? I don't believe we have changed any code recently in NotifyListener. I see pmonette@chromium.org making some changes in that method last year. Is this bug related to those changes?

Comment 15 by hardi...@google.com on Tue, Mar 22, 2022, 11:37 PM EDT

Cc: pmonette@chromium.org

Comment 16 by pmonette@google.com on Wed, Mar 23, 2022, 1:15 AM EDT

The ScanningHandler and the CupsPrinterHandler code need a guard against opening a SelectFileDialog while one is already open, akin to this fix: https://chromium-review.googlesource.com/c/chromium/src/+/2898617

Comment 17 by vulb...@gmail.com on Wed, Mar 23, 2022, 1:19 AM EDT

#c16 Yes, I also think so.

Comment 18 by pmonette@google.com on Wed, Mar 23, 2022, 3:16 PM EDT

Cc: zentaro@chromium.org

+zentaro who will be reviewing my fix.

Comment 19 by majewski@chromium.org on Wed, Mar 23, 2022, 11:00 PM EDT

Cc: lucmult@chromium.org

Comment 20 by Git Watcher on Fri, Mar 25, 2022, 5:13 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/004c2a28c015c658b5e5f7bcb19c9b7910135cc6

commit 004c2a28c015c658b5e5f7bcb19c9b7910135cc6
Author: Patrick Monette <pmonette@chromium.org>
Date: Fri Mar 25 21:12:41 2022

Prevent the creation of a duplicate dialog in CupsPrintersHandler

~~Bug: 1306391~~
Change-Id: Iab82abfed428b1040671bcede0ddaf9e682552b5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3546821
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Commit-Position: refs/heads/main@{#985491}

[modify]
https://crrev.com/004c2a28c015c658b5e5f7bcb19c9b7910135cc6/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.h
[modify]
https://crrev.com/004c2a28c015c658b5e5f7bcb19c9b7910135cc6/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.cc

Comment 21 by Git Watcher on Fri, Mar 25, 2022, 5:56 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b7209bc027a96c83473ea6390ffbef3550e3860d

commit b7209bc027a96c83473ea6390ffbef3550e3860d
Author: Patrick Monette <pmonette@chromium.org>
Date: Fri Mar 25 21:55:11 2022

Prevent the creation of a duplicate dialog in ScanningHandler

~~Bug: 1306391~~
Change-Id: I315ca8f8d6ce368f0cdf56956c1dc79a9805547e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3545287
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Commit-Position: refs/heads/main@{#985509}

[modify] https://crrev.com/b7209bc027a96c83473ea6390ffbef3550e3860d/ash/webui/scanning/scanning_handler.cc
[modify]
https://crrev.com/b7209bc027a96c83473ea6390ffbef3550e3860d/ash/webui/scanning/scanning_handler_unittest.cc

Comment 22 by sheriffbot on Tue, Apr 5, 2022, 12:21 PM EDT

gavinwill: 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 lucmult@chromium.org on Tue, Apr 5, 2022, 7:27 PM EDT

Status: Started (was: Assigned)
Owner: lucmult@chromium.org
Blockedon: 1309583

I'm working on fixing the caller sites of SelectFileDialog and I'm tracking the work on crbug.com/1309583

Comment 24 by lucmult@chromium.org on Thu, Apr 7, 2022, 2:05 AM EDT

Status: Fixed (was: Started)

All the uses of SelectFileDialog mentioned in this bug have been fixed.

Comment 25 by sheriffbot on Thu, Apr 7, 2022, 12:42 PM EDT

Labels: reward-topanel

Comment 26 by sheriffbot on Thu, Apr 7, 2022, 1:41 PM EDT

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

Comment 27 by amyressler@chromium.org on Mon, Apr 11, 2022, 5:32 PM EDT

Note for VRP Panel: according to https://bugs.chromium.org/p/chromium/issues/detail?id=1304884#c14 this issue is a duplicate of earlier reported ~~issue 1304884~~, which should be considered for the potential VRP Reward. This bug cannot be merged into the earlier report as the fix CLs were associated with this report.

Comment 28 by amyressler@chromium.org on Mon, Apr 11, 2022, 5:34 PM EDT

Labels: FoundIn-100

Comment 29 by amyressler@chromium.org on Mon, Apr 11, 2022, 5:37 PM EDT

Labels: FoundIn-98 FoundIn-99

Added FoundIn-100 to reflect current security-imact == Extended Stable; adding foundin-98 and foundin-99 to ensure this doesn't appear to be regression to sheriffbot or any else based on fixed/CL landing dates

Comment 30 by sheriffbot on Tue, Apr 12, 2022, 12:51 PM EDT

Labels: M-101 Target-101

Setting milestone and target because of medium severity.

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

Comment 31 by sheriffbot on Tue, Apr 12, 2022, 2:06 PM EDT

Labels: Merge-Request-101

Requesting merge to beta M101 because latest trunk commit (985509) appears to be after beta branch point (982481).

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

Comment 32 by sheriffbot on Tue, Apr 12, 2022, 2:10 PM EDT

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

Merge review required: M101 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 33 by matthewjoseph@google.com on Tue, Apr 12, 2022, 3:59 PM EDT

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

Merge approved, 101

Comment 34 by amyressler@chromium.org on Tue, Apr 12, 2022, 9:30 PM EDT

Labels: Security_Impact-Extended

Comment 35 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 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. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 36 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:29 PM EDT

Hello and thank you for your report! As your report was a duplicate of a previously reported issue, it would generally be ineligible for a VRP reward. However, due to the extra information and stack trace that allowed this issue to be reproduced, triaged, and fixed faster, we did want to extend a thank you, in the form of a $1,000 reward. Thank you for your efforts and reporting this issue to us.

Comment 37 by amyressler@google.com on Fri, Apr 15, 2022, 9:50 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 38 by sheriffbot on Mon, Apr 18, 2022, 12:22 PM EDT

Cc: matthewjoseph@google.com

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 39 by Git Watcher on Mon, Apr 18, 2022, 8:25 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/588c2b08e2f4f3d6b6f23c01464192f5d21eacba

commit 588c2b08e2f4f3d6b6f23c01464192f5d21eacba
Author: Patrick Monette <pmonette@chromium.org>
Date: Tue Apr 19 00:24:41 2022

M101: Prevent the creation of a duplicate dialog in CupsPrintersHandler

(cherry picked from commit 004c2a28c015c658b5e5f7bcb19c9b7910135cc6)

~~Bug: 1306391~~
Change-Id: Iab82abfed428b1040671bcede0ddaf9e682552b5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3546821
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>

Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985491}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3582440
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Reviewed-by: Patrick Monette <pmonette@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#866}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/588c2b08e2f4f3d6b6f23c01464192f5d21eacba/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.h
[modify]
https://crrev.com/588c2b08e2f4f3d6b6f23c01464192f5d21eacba/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.cc

Comment 40 by Git Watcher on Mon, Apr 18, 2022, 8:25 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bccb5551a84b695377910d186105c5555834f96e

commit bccb5551a84b695377910d186105c5555834f96e
Author: Patrick Monette <pmonette@chromium.org>
Date: Tue Apr 19 00:24:16 2022

M101: Prevent the creation of a duplicate dialog in ScanningHandler

(cherry picked from commit b7209bc027a96c83473ea6390ffbef3550e3860d)

~~Bug: 1306391~~
Change-Id: I315ca8f8d6ce368f0cdf56956c1dc79a9805547e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3545287
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985509}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3583877
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Reviewed-by: Patrick Monette <pmonette@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#865}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify] https://crrev.com/bccb5551a84b695377910d186105c5555834f96e/ash/webui/scanning/scanning_handler.cc
[modify]
https://crrev.com/bccb5551a84b695377910d186105c5555834f96e/ash/webui/scanning/scanning_handler_unittest.cc

Comment 41 by sheriffbot on Mon, Apr 18, 2022, 8:30 PM EDT

Labels: LTS-Merge-Candidate

LTS Milestone M96

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

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

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

Comment 42 by rzanoni@google.com on Tue, Apr 19, 2022, 1:15 PM EDT

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

Comment 43 by rzanoni@google.com on Tue, Apr 19, 2022, 2:49 PM EDT

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

Comment 44 by sheriffbot on Tue, Apr 19, 2022, 2:49 PM EDT

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

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

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

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

Comment 45 by rzanoni@google.com on Tue, Apr 19, 2022, 2:51 PM EDT

1. Just https://crrev.com/c/3593966
2. Low, simple conflict with the arguments of CupsPrintersHandler::HandleSelectPPDFile
3. 101
4. Yes

Comment 46 by gmpritchard@google.com on Wed, Apr 20, 2022, 12:56 PM EDT

Labels: LTS-Merge-Delayed-96

Comment 47 by gmpritchard@google.com on Wed, Apr 20, 2022, 1:02 PM EDT

Labels: -LTS-Merge-Candidate

Comment 48 by gmpritchard@google.com on Fri, Apr 22, 2022, 1:20 PM EDT

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

Comment 49 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:03 PM EDT

Labels: Release-0-M101

Comment 50 by Git Watcher on Tue, Apr 26, 2022, 10:29 AM EDT

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6a2190a8566a1c8e58155eb85420bbb769a00803

commit 6a2190a8566a1c8e58155eb85420bbb769a00803
Author: Patrick Monette <pmonette@chromium.org>
Date: Tue Apr 26 14:28:54 2022

[M96-LTS] Prevent the creation of a duplicate dialog in CupsPrintersHandler

M96 merge issues:
cups_printers_handler.cc:
- CupsPrintersHandler::HandleSelectPPDFile paramenter "args" isn't a reference in M96

(cherry picked from commit 004c2a28c015c658b5e5f7bcb19c9b7910135cc6)

~~Bug: 1306391~~
Change-Id: Iab82abfed428b1040671bcede0ddaf9e682552b5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3546821
Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985491}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3593966
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1605}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/6a2190a8566a1c8e58155eb85420bbb769a00803/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.h
[modify]
https://crrev.com/6a2190a8566a1c8e58155eb85420bbb769a00803/chrome/browser/ui/webui/settings/chromeos/cups_printers_handler.cc

Comment 51 by rzanoni@google.com on Tue, Apr 26, 2022, 12:29 PM EDT

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

Comment 52 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT

Labels: CVE-2022-1496 CVE_description-missing

Comment 53 by rzanoni@google.com on Wed, Apr 27, 2022, 12:02 PM EDT

Labels: -LTS-Merge-Merged-96 LTS-Merge-Candidate LTS-Evaluating-96

Adding LTS-Merge-Candidate back because I skipped https://crrev.com/c/3611127

Comment 54 by rzanoni@google.com on Wed, Apr 27, 2022, 2:50 PM EDT

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

Comment 55 by sheriffbot on Wed, Apr 27, 2022, 2:51 PM EDT

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

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

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

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

Comment 56 Deleted

Comment 57 by rzanoni@google.com on Thu, Apr 28, 2022, 10:48 AM EDT

1. Just https://crrev.com/c/3611127
2. Low, just a simple conflict with the way the argument list is checked on the changed code
3. 101
4. Yes

Comment 58 by gmpritchard@google.com on Mon, May 2, 2022, 12:34 PM EDT

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

Comment 59 by Git Watcher on Tue, May 3, 2022, 9:17 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1c4f05e0cf217f48541ff490673664a37e8ad53a

commit 1c4f05e0cf217f48541ff490673664a37e8ad53a
Author: Patrick Monette <pmonette@chromium.org>
Date: Tue May 03 13:16:36 2022

[M96-LTS] Prevent the creation of a duplicate dialog in ScanningHandler

M96 merge issues:
scanning_handler.cc:
Conflicting ways of checking the args list

(cherry picked from commit b7209bc027a96c83473ea6390ffbef3550e3860d)

~~Bug: 1306391~~
Change-Id: I315ca8f8d6ce368f0cdf56956c1dc79a9805547e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3545287
Commit-Queue: Patrick Monette <pmonette@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#985509}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3611127
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1612}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/1c4f05e0cf217f48541ff490673664a37e8ad53a/ash/webui/scanning/scanning_handler.cc
[modify] https://crrev.com/1c4f05e0cf217f48541ff490673664a37e8ad53a/ash/webui/scanning/scanning_handler_unittest.cc

Comment 60 by rzanoni@google.com on Tue, May 3, 2022, 9:19 AM EDT

Labels: -LTS-Merge-Approved-96 LTS-Merged-90

Comment 61 by rzanoni@google.com on Tue, May 3, 2022, 9:19 AM EDT

Labels: -LTS-Merged-90 LTS-Merge-Merged-96

Comment 62 by sheriffbot on Thu, Jul 14, 2022, 1:32 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 63 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 64 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing