Starred by 3 users

Owner:	lucmult@chromium.org
CC:	simmonsjosh@google.com rzanoni@google.com lucmult@chromium.org ajgo@google.com jimmyxgong@chromium.org majewski@chromium.org jamescook@chromium.org dcheng@chromium.org sky@chromium.org gavinwill@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Apps>FileManager
Modified:	Oct 18, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

M-100
reward-5000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-100
FoundIn-99
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-100
merge-merged-4951
merge-merged-101
Release-1-M101
CVE-2022-1641

BlockedOn: Issue 922327

View details

Issue 1305068: Security: UAF in SelectFileDialogExtension::NotifyListener

Reported by jtrro...@gmail.com on Thu, Mar 10, 2022, 12:02 AM EST

Code

VULNERABILITY DETAILS

SelectFileDialog::Create returns a scoped_refptr to a ref-counted SelectFileDialog instance. Usually one reference is owned by the class which extends SelectFileDialog::Listener and creates the dialog. And other references may also be retained elsewhere. On ChromeOS, for example, it calls SelectFileDialogExtension::AddPending to add the dialog instance to PendingDialog map [1].

When the dialog is cloing, SelectFileDialogExtension::ExtensionDialogClosing will be invoked which would remove the reference in PendingDialog map [2]. However, If there is no other reference at this time, this instance will be immediately destroyed, thus causing UAF in function SelectFileDialogExtension::NotifyListener [3].

```
void SelectFileDialogExtension::SelectFileWithFileManagerParams(
    Type type,
    const std::u16string& title,
    const base::FilePath& default_path,
    const FileTypeInfo* file_types,
    int file_type_index,
    void* params,
    const Owner& owner,
    const std::string& search_query,
    bool show_android_picker_apps) {
  // skip

  // Connect our listener to FileDialogFunction's per-tab callbacks.
  AddPending(routing_id);    // ===> [1]

  params_ = params;
  routing_id_ = routing_id;
  owner_window_ = owner.window;
}

void SelectFileDialogExtension::ExtensionDialogClosing(
    ExtensionDialog* /*dialog*/) {
  if (!ash::features::IsFileManagerSwaEnabled() && ash::ColorProvider::Get())
    ash::ColorProvider::Get()->RemoveObserver(this);
  profile_ = nullptr;
  owner_window_ = nullptr;
  // Release our reference to the underlying dialog to allow it to close.
  extension_dialog_ = nullptr;
  system_files_app_web_contents_ = nullptr;
  PendingDialog::GetInstance()->Remove(routing_id_);    // ===> [2]
  // Actually invoke the appropriate callback on our listener.
  NotifyListener();
}

void SelectFileDialogExtension::NotifyListener() {
```

```
  if (!listener_)    // ===> [3]
    return;
  // skip
}
```

[1]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=532;drc=214db6b05f61309e14eab393755ca3ab47857012
[2]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=291;drc=214db6b05f61309e14eab393755ca3ab47857012
[3]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=566;drc=214db6b05f61309e14eab393755ca3ab47857012

It seems there are several cases using SelectFileDialog may trigger the UAF, such as CertificatesHandler, SessionLogHandler, CupsPrintersHandler and ScanningHandler. Take CertificatesHandler as example, if attacker calls CertificatesHandler::HandleImportServer twice, the reference to the dialog opened at the first time would be dropped at [4], which leads to UAF when the dialog is closed.

```
void CertificatesHandler::HandleImportServer(const base::Value::List& args) {
  CHECK_EQ(1U, args.size());
  AssignWebUICallbackId(args);

  select_file_dialog_ = ui::SelectFileDialog::Create(    // ===> [4]
      this,
      std::make_unique<ChromeSelectFilePolicy>(web_ui()->GetWebContents()));
  ShowCertSelectFileDialog(
      select_file_dialog_.get(), ui::SelectFileDialog::SELECT_OPEN_FILE,
      base::FilePath(), GetParentWindow(),
      reinterpret_cast<void*>(IMPORT_SERVER_FILE_SELECTED));
}
```

[4]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/webui/certificates_handler.cc;l=752;drc=58a9db5dc15b120154849f793ccde830ea8cfc27

VERSION
Chrome Version: stable
Operating System: ChromeOS (Maybe it would affect other platforms)

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser

Comment 1 by sheriffbot on Thu, Mar 10, 2022, 12:04 AM EST Project Member

Labels: external_security_report

Comment 2 by jtrro...@gmail.com on Thu, Mar 10, 2022, 7:31 AM EST

REPRODUCTION CASE
I think the quick way to demonstrate is sending message from Dev tools directly. Take ScanningHandler as example:

1. Open Scan app on ChromeOS (navigate to chrome://scanning or open it from Launcher).
2. Open Dev tools (press F12 or right-click then select inspect)
3. Run following js codes
chrome.send("requestScanToLocation", [""]); chrome.send("requestScanToLocation", [""]);
4. Close the dialog

Another possible way to reproduce is to use extension detailed in issue https://bugs.chromium.org/p/chromium/issues/detail?id=1201032#c39. It does not require access to Dev tools, but needs more user interaction.

FIX
It might be a good idea to check whether a dialog already exists before creating a new one, and get rid of the reference explicitly when the dialog finishes its job. For example, in NetExportMessageHandler::ShowSelectFileDialog:

```
void NetExportMessageHandler::ShowSelectFileDialog(
    const base::FilePath& default_path) {
  // User may have clicked more than once before the save dialog appears.
  // This prevents creating more than one save dialog.
  if (select_file_dialog_)
    return;

  // skip
}

void NetExportMessageHandler::FileSelected(const base::FilePath& path,
                                           int index,
                                           void* params) {
  // skip

  // IMPORTANT: resetting the dialog may lead to the deletion of |path|, so keep
  // this line last.
  select_file_dialog_ = nullptr;
}
```

Comment 3 by jtrro...@gmail.com on Thu, Mar 10, 2022, 7:32 AM EST

asan.log
27.1 KB View Download

Comment 4 by bookholt@chromium.org on Thu, Mar 10, 2022, 7:10 PM EST Project Member

Status: Duplicate (was: Unconfirmed)
Mergedinto: 1304145

Comment 5 by jtrro...@gmail.com on Thu, Mar 10, 2022, 10:46 PM EST

I don't have permission to access ~~issue 1304145~~, but according to the fix code (https://chromium-review.googlesource.com/c/chromium/src/+/3517546), this issue is not the same problem as 1304145. It would be great if you could reconsider this, thank you.

Comment 6 by adetaylor@google.com on Thu, Mar 17, 2022, 3:54 PM EDT Project Member

Status: Unconfirmed (was: Duplicate)

Reopening for reconsideration by current sheriff.

Comment 7 by thestig@chromium.org on Mon, Mar 21, 2022, 1:25 PM EDT Project Member

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

+folks from ~~bug 1304145~~.

Comment 8 by thestig@chromium.org on Mon, Mar 21, 2022, 1:28 PM EDT Project Member

Cc: majewski@chromium.org
Labels: OS-Chrome
Components: Platform>Apps>FileManager

Comment 9 by aashay@google.com on Wed, Mar 23, 2022, 4:26 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: majewski@chromium.org
Labels: Security_Impact-Stable FoundIn-99 Security_Severity-Medium Pri-1

Comment 10 by majewski@chromium.org on Wed, Mar 23, 2022, 8:53 PM EDT Project Member

Cc: simmonsjosh@google.com

Comment 11 by majewski@chromium.org on Wed, Mar 23, 2022, 9:03 PM EDT Project Member

This seems to be related to ~~crbug.com/1306391~~

Comment 12 by simmonsjosh@google.com on Wed, Mar 23, 2022, 10:30 PM EDT Project Member

Owner: lucmult@chromium.org
Cc: lucmult@chromium.org

Comment 13 by lucmult@chromium.org on Wed, Mar 23, 2022, 11:07 PM EDT Project Member

Blockedon: 922327

Thanks for the detailed report.

I investigated something similar in the past and couldn't get a definitive fix at the time, from the crash reports from here: https://bugs.chromium.org/p/chromium/issues/detail?id=922327

For some reason I can't reproduce this error on my local linux-chromeos environment, but using a device on dev channel I can still reproduce the crash.

The suggestions in #2 and #5 might fix some caller sites, but I recommend we fix SelectFileDialogExtension, right now the code assumes that a given WebContents can only have 1 dialog, whereas there is no such guarantee in the code, as this reports demonstrates. :-)

Right now SelectFileDialogExtension::RoutingID identifies a WebContents (or an Android app), whereas we have to identify each SelectFileDialog in a given WebContents (or Android app).

Fixing this way even if a WebContents spawns multiple SelectFileDialog we shouldn't cause a UAF.

I'll check the code history to see if there is a reason for assuming only 1 dialog per WebContents.

Comment 14 by lucmult@chromium.org on Wed, Mar 23, 2022, 11:19 PM EDT Project Member

Status: Started (was: Assigned)
Cc: jamescook@chromium.org sky@chromium.org

CCing jamescook@ and sky@ who have been around this code a few times too.

Do you know if we have any reason to limit one SelectFileDialog per WebContents? This assumption is baked in in [1], so if an client Dialog spawns 2 SelectFileDialogs (see #2) then closing 1 dialog leaves a invalid pointer in the other dialog.

I'm considering adding a static counter in the GetRoutingID() so we identify each SelectFileDialog instance to fix this.

[1] - https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/select_file_dialog_extension.cc;l=166-182;drc=214db6b05f61309e14eab393755ca3ab47857012

Comment 15 by lucmult@chromium.org on Thu, Mar 24, 2022, 12:38 AM EDT Project Member

Changing SelectFileDialogExtension (patchset #1):
https://chromium-review.googlesource.com/c/chromium/src/+/3545992/1

However this doesn't fix the crash reported here because each ScanningHandler dangles its pointer to SelectFileDialog, so we need to audit all caller sites to ui::SelectFileDialog::Create(). Fixing the ScanningHandler (patchset #2):
https://chromium-review.googlesource.com/c/chromium/src/+/3545992/2

Comment 16 by lucmult@chromium.org on Thu, Mar 24, 2022, 1:24 AM EDT Project Member

I started a internal spreadsheet to track all the current call sites.
https://docs.google.com/spreadsheets/d/1yiFNwmXb1_Dc9JKyG4iDTcYRT5OvrQtdu8rR7wU_sBc/edit#gid=0

Comment 17 by jamescook@chromium.org on Thu, Mar 24, 2022, 11:39 AM EDT Project Member

Re: comment 14 - I don't remember a particular reason why we limit to one SelectFileDialog per WebContents. I suspect that assumption has been baked in for many years, but it might just be a mistake.

Comment 18 by sheriffbot on Thu, Mar 24, 2022, 12:52 PM EDT Project Member

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 19 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 20 by Git Watcher on Thu, Mar 31, 2022, 7:00 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a7a8ff2579e4dd47f5c97ad2482fb2149d950bab

commit a7a8ff2579e4dd47f5c97ad2482fb2149d950bab
Author: Luciano Pacheco <lucmult@chromium.org>
Date: Thu Mar 31 22:59:23 2022

Prevent multiple SelectFileDialog in SessionLogHandler

Similar to crrev.com/c/3546821

~~Bug: 1305068~~
Change-Id: I5d7cb86d868e31683db94249a3896448178bd334
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3561204
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Commit-Position: refs/heads/main@{#987684}

[modify]
https://crrev.com/a7a8ff2579e4dd47f5c97ad2482fb2149d950bab/ash/webui/diagnostics_ui/backend/session_log_handler.cc

Comment 21 by ajgo@google.com on Wed, Apr 6, 2022, 12:13 AM EDT Project Member

Cc: ajgo@google.com jimmyxgong@chromium.org

~~Issue 1305906~~ has been merged into this issue.

Comment 22 by lucmult@chromium.org on Thu, Apr 7, 2022, 2:02 AM EDT Project Member

Status: Fixed (was: Started)

CertificateHandler has been fixed on:
https://chromium-review.googlesource.com/c/chromium/src/+/3573861

All uses of SelectFileDialog reported in this bug are fixed now.

Comment 23 by sheriffbot on Thu, Apr 7, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 24 by sheriffbot on Thu, Apr 7, 2022, 1:41 PM EDT Project Member

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

Comment 25 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 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 26 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:25 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $5,000 for this report. As this issue is mitigated by significant user interaction and is receiving a reduced reward amount, the reward amount is higher than that of other issues of this class of non-web accessible bugs as your report did lead to our teams finding other instances of this issue. Thank you for your additional analysis and reporting this issue to us!

Comment 27 by amyressler@google.com on Fri, Apr 15, 2022, 9:48 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 28 by Git Watcher on Tue, Apr 26, 2022, 12:24 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/28e187eaf9ca08ee638978e0fcf065bbde2d6a78

commit 28e187eaf9ca08ee638978e0fcf065bbde2d6a78
Author: Luciano Pacheco <lucmult@chromium.org>
Date: Tue Apr 26 04:23:44 2022

M101: Prevent multiple SelectFileDialog in SessionLogHandler

Similar to crrev.com/c/3546821

(cherry picked from commit a7a8ff2579e4dd47f5c97ad2482fb2149d950bab)

~~Bug: 1305068~~
Change-Id: I5d7cb86d868e31683db94249a3896448178bd334
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3561204
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#987684}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3581507
Commit-Queue: Luciano Pacheco <lucmult@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#1054}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/28e187eaf9ca08ee638978e0fcf065bbde2d6a78/ash/webui/diagnostics_ui/backend/session_log_handler.cc

Comment 29 by sheriffbot on Tue, Apr 26, 2022, 12:27 AM EDT Project Member

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 30 by Git Watcher on Tue, Apr 26, 2022, 12:14 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0f6c9878641be05f3b126bff2da53f68def8af1a

commit 0f6c9878641be05f3b126bff2da53f68def8af1a
Author: Luciano Pacheco <lucmult@chromium.org>
Date: Tue Apr 26 16:13:11 2022

M100: Prevent multiple SelectFileDialog in SessionLogHandler

Similar to crrev.com/c/3546821

(cherry picked from commit a7a8ff2579e4dd47f5c97ad2482fb2149d950bab)

~~Bug: 1305068~~, 1309583
Change-Id: I5d7cb86d868e31683db94249a3896448178bd334
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3561204
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Reviewed-by: Zentaro Kavanagh <zentaro@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#987684}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3606672
Cr-Commit-Position: refs/branch-heads/4896@{#1186}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/0f6c9878641be05f3b126bff2da53f68def8af1a/ash/webui/diagnostics_ui/backend/session_log_handler.cc

Comment 31 by rzanoni@google.com on Tue, Apr 26, 2022, 5:11 PM EDT Project Member

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

Comment 32 by rzanoni@google.com on Wed, Apr 27, 2022, 11:03 AM EDT Project Member

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

Comment 33 by sheriffbot on Wed, Apr 27, 2022, 11:08 AM EDT Project Member

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 34 by rzanoni@google.com on Wed, Apr 27, 2022, 11:10 AM EDT Project Member

1. Just https://crrev.com/c/3609031
2. Low, no conflicts
3. 100, 101
4. Yes

Comment 35 by gmpritchard@google.com on Thu, Apr 28, 2022, 10:35 AM EDT Project Member

Labels: -LTS-Merge-Candidate -LTS-Merge-Review-96 -merge-merged-4896 LTS-Merge-Approved-96

Comment 36 by Git Watcher on Wed, May 4, 2022, 10:10 AM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/097594adb58d997cd7770792c571361297a2cafb

commit 097594adb58d997cd7770792c571361297a2cafb
Author: Luciano Pacheco <lucmult@chromium.org>
Date: Wed May 04 14:09:01 2022

[M96-LTS] Prevent multiple SelectFileDialog in SessionLogHandler

Similar to crrev.com/c/3546821

(cherry picked from commit a7a8ff2579e4dd47f5c97ad2482fb2149d950bab)

~~Bug: 1305068~~
Change-Id: I5d7cb86d868e31683db94249a3896448178bd334
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3561204
Auto-Submit: Luciano Pacheco <lucmult@chromium.org>
Commit-Queue: Zentaro Kavanagh <zentaro@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#987684}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3609031
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1616}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]

https://crrev.com/097594adb58d997cd7770792c571361297a2cafb/ash/webui/diagnostics_ui/backend/session_log_handler.cc

Comment 37 by rzanoni@google.com on Wed, May 4, 2022, 12:14 PM EDT Project Member

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

Comment 38 by amyressler@chromium.org on Mon, May 9, 2022, 12:59 PM EDT Project Member

Labels: Release-1-M101

Comment 39 by amyressler@google.com on Mon, May 9, 2022, 1:38 PM EDT Project Member

Labels: CVE-2022-1641 CVE_description-missing

Comment 40 by sheriffbot on Thu, Jul 14, 2022, 1:32 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 41 by amyressler@google.com on Tue, Jul 26, 2022, 5:59 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 42 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

Comment 43 by chromeos-software-bugbot on Mon, Oct 17, 2022, 8:12 PM EDT Project Member

Labels: sw-b-migration-candidate

Comment 44 by simmonsjosh@google.com on Tue, Oct 18, 2022, 3:07 AM EDT Project Member

Labels: -sw-b-migration-candidate