Starred by 3 users

Owner:	dtapu...@chromium.org
CC:	rzanoni@google.com bartekn@chromium.org mcnee@chromium.org haraken@chromium.org adithyas@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions UI>Browser>Navigation
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Severity-High
allpublic
CVE_description-submitted
M-98
Target-98
FoundIn-96
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
LTS-Merge-Merged-96
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0972

Issue 1301320: Security: heap-use-after-free in extensions::ExtensionApiFrameIdMap::GetFrameId

Reported by glazunov@google.com on Mon, Feb 28, 2022, 8:11 AM EST Project Member

Code

SUMMARY

A use-after-free issue exists in Chrome 100 and earlier versions. A malicious extension can achieve arbitrary code execution in the browser process.

VULNERABILITY DETAILS

```
// A handler for a single injection request. On creation this will send the
// injection request to the renderer, and it will be destroyed after either the
// corresponding response comes from the renderer, or the renderer is destroyed.
class Handler : public content::WebContentsObserver {
[...]
  Handler(base::PassKey<ScriptExecutor> pass_key,
          ScriptsExecutedOnceCallback observer,
          content::WebContents* web_contents,
          mojom::ExecuteCodeParamsPtr params,
          ScriptExecutor::FrameScope scope,
          const std::set<int>& frame_ids,
          ScriptExecutor::ScriptFinishedCallback callback) {
[...]
    // If we are to include subframes, iterate over all descendants of frames in
    // `pending_render_frames_` and add them if they are alive (and not already
    // contained in `pending_frames`).
    if (scope == ScriptExecutor::INCLUDE_SUB_FRAMES) {
      auto append_frame =
          [](std::vector<content::RenderFrameHost*>* pending_frames,
             content::RenderFrameHost* frame) {
            if (!frame->IsRenderFrameLive() ||
                base::Contains(*pending_frames, frame)) {
              return;
            }

            pending_frames->push_back(frame);
          };

      // We iterate over the requested frames. Note we can't use an iterator
      // as the for loop will mutate `pending_render_frames_`.
      size_t requested_frame_count = pending_render_frames_.size();
      for (size_t i = 0; i < requested_frame_count; ++i) {
        auto* frame = pending_render_frames_.at(i);
        frame->ForEachRenderFrameHost( // *** 1 ***
            base::BindRepeating(append_frame, &pending_render_frames_));
      }

    }

    for (content::RenderFrameHost* frame : pending_render_frames_) {
```

```
    for (content::RenderFrameHost* frame : pending_render_frames_)
      SendExecuteCode(pass_key, params.Clone(), frame);

    if (pending_render_frames_.empty())
      Finish();
  }
[...]
  void WebContentsDestroyed() override {
    for (content::RenderFrameHost* frame : pending_render_frames_) {
      int frame_id = ExtensionApiFrameIdMap::GetFrameId(frame); // *** 2 ***
      AddWillNotInjectResult(
          frame_id,
          base::StringPrintf("Tab containing frame with ID %d was removed.",
                             frame_id));
    }
    pending_render_frames_.clear();
    Finish();
  }
[...]
  void RenderFrameDeleted(
      content::RenderFrameHost* render_frame_host) override {
    int erased_count = base::Erase(pending_render_frames_, render_frame_host); // *** 3 ***
[...]
  }
```

This issue is almost identical to ~~https://crbug.com/1284367~~. The `Handler` constructor calls `ForEachRenderFrameHost` to make a list of the frames in a given tab[1], including frames that belong to nested `WebContents` objects, and listens to the `RenderFrameDeleted` event to remove old frames from the list[3]. Unfortunately, `RenderFrameDeleted` doesn't get triggered for nested `WebContents` frames, so the `pending_render_frames_` list may end up with dangling pointers to such frames, which will get dereferenced when the tab is closed[2].

VERSION
98.0.4758.109 (Official Build) (arm64)
100.0.4893.0 (Developer Build) (64-bit)

REPRODUCTION CASE
A browser extension with the "scripting" permission can exploit the bug to escape the sandbox. To reproduce:
1. Make repro.html available at http://localhost:8000/repro.html.
2. Load the attached unpacked extension via chrome://extensions/.

Alternatively, a malicious web page can target users of popular extensions that rely on the `executeScript` API.

CREDIT INFORMATION
Sergei Glazunov of Google Project Zero

available. Otherwise, this bug report will become public at the deadline.
The scheduled deadline is 2022-05-29.

asan.log
26.9 KB View Download

manifest.json
218 bytes View Download

repro.html
174 bytes View Download

sw.js
445 bytes View Download

Comment 1 by dcheng@chromium.org on Wed, Mar 2, 2022, 12:56 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: dtapu...@chromium.org
Labels: Security_Severity-Critical FoundIn-96 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-0
Components: Platform>Extensions

Comment 2 by dcheng@chromium.org on Wed, Mar 2, 2022, 12:59 AM EST Project Member

I've also pinged the mparch team to let them know about this issue: this seems like something that could happen quite easily with anything that combines ForEachRenderFrameHost() and WebContentsObserver::RenderFrameDeleted().

Comment 3 by sheriffbot on Wed, Mar 2, 2022, 1:04 AM EST Project Member

Labels: Security_Impact-Extended

Comment 4 by dcheng@chromium.org on Wed, Mar 2, 2022, 12:20 PM EST Project Member

Cc: adithyas@chromium.org

Comment 5 by dcheng@chromium.org on Wed, Mar 2, 2022, 12:33 PM EST Project Member

Cc: mcnee@chromium.org

Comment 6 by sheriffbot on Wed, Mar 2, 2022, 12:47 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 7 by creis@chromium.org on Fri, Mar 4, 2022, 1:58 PM EST Project Member

Components: UI>Browser>Navigation

dtapuska@ / mcnee@: Any updates on this that you can post? Do we need to audit additional ForEachRenderFrameHost cases as well? Thanks!

Comment 8 by dtapu...@chromium.org on Fri, Mar 4, 2022, 2:12 PM EST Project Member

Change is here... https://chromium-review.googlesource.com/c/chromium/src/+/3497565 Just waiting on Kevin to stamp the

raw_ptr change he requested.

Comment 9 by Git Watcher on Fri, Mar 4, 2022, 2:44 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5c4e043324b3afd1be673ae2c0a5c00845bb0e86

commit 5c4e043324b3afd1be673ae2c0a5c00845bb0e86
Author: Dave Tapuska <dtapuska@chromium.org>
Date: Fri Mar 04 19:43:47 2022

Do not expose inner WebContents on scripting/getAllFrames.

Inner WebContents shouldn't be exposed for executeScript or getAllFrames
APIs. This is consistent with the API before crrev.com/f894f106
and crrev.com/c8de3b0a.

~~BUG=1301320~~,1261261

Change-Id: I86a5b09aa44c48319b7dd0a10e5442b8c803d4e5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Dave Tapuska <dtapuska@chromium.org>
Cr-Commit-Position: refs/heads/main@{#977769}

[modify] https://crrev.com/5c4e043324b3afd1be673ae2c0a5c00845bb0e86/extensions/browser/script_executor.cc
[modify]
https://crrev.com/5c4e043324b3afd1be673ae2c0a5c00845bb0e86/chrome/browser/extensions/api/scripting/scripting_apitest.cc
[add]
https://crrev.com/5c4e043324b3afd1be673ae2c0a5c00845bb0e86/chrome/test/data/extensions/api_test/scripting/nested_web_contents/worker.js
[modify]
https://crrev.com/5c4e043324b3afd1be673ae2c0a5c00845bb0e86/chrome/browser/extensions/api/web_navigation/web_navigation_api.cc
[add]
https://crrev.com/5c4e043324b3afd1be673ae2c0a5c00845bb0e86/chrome/test/data/extensions/api_test/scripting/nested_web_contents/manifest.json

Comment 10 by dtapu...@chromium.org on Fri, Mar 4, 2022, 2:45 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 11 by mcnee@chromium.org on Fri, Mar 4, 2022, 4:25 PM EST Project Member

creis: I looked through ForEachRenderFrameHost callers looking for callbacks that produce long lived raw RenderFrameHost pointers that warrant follow up. See issue 1303124.

Comment 12 by sheriffbot on Sat, Mar 5, 2022, 1:40 PM EST Project Member

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

Comment 13 by sheriffbot on Sat, Mar 5, 2022, 2:00 PM EST Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (977769) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (977769) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (977769) appears to be after beta branch point (972766).

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

Comment 14 by sheriffbot on Sat, Mar 5, 2022, 2:49 PM EST Project Member

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

Merge review required: M100 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: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 15 by sheriffbot on Sat, Mar 5, 2022, 2:49 PM EST Project Member

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

Merge review required: M99 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: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

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

Comment 16 by sheriffbot on Sat, Mar 5, 2022, 2:49 PM EST Project Member

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

Merge review required: M98 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), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 17 by dtapu...@chromium.org on Mon, Mar 7, 2022, 11:50 AM EST Project Member

1. Yes. M98-M100
2. https://chromium-review.googlesource.com/c/chromium/src/+/3497565
3. Yes 101.0.4925.0 and later
4. No
5. No
6. Yes, see repro tests loading unpacked extension in Comment #0

Comment 18 by srinivassista@google.com on Mon, Mar 7, 2022, 12:36 PM EST Project Member

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

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

Comment 19 by srinivassista@google.com on Mon, Mar 7, 2022, 2:55 PM EST Project Member

This bug is approved for M100 merge, please complete your merge asap so this can be included in the beta release this week. Beta RC will be cut tomorrow (tuesday) March 8th at 3pm PST [Bulk Update]

Comment 20 by Git Watcher on Tue, Mar 8, 2022, 1:15 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec

commit 382ed1260b5eb60a8bfe9847ce6d2095f2f544ec
Author: Dave Tapuska <dtapuska@chromium.org>
Date: Tue Mar 08 18:14:46 2022

Do not expose inner WebContents on scripting/getAllFrames.

Inner WebContents shouldn't be exposed for executeScript or getAllFrames

inner WebContents shouldn't be exposed for executeScript or getAllFrames APIs. This is consistent with the API before crrev.com/f894f106 and crrev.com/c8de3b0a.

~~BUG=1301320~~,1261261

(cherry picked from commit 5c4e043324b3afd1be673ae2c0a5c00845bb0e86)

Change-Id: I86a5b09aa44c48319b7dd0a10e5442b8c803d4e5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Dave Tapuska <dtapuska@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977769}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3507493
Auto-Submit: Dave Tapuska <dtapuska@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Owners-Override: Prudhvikumar Bommana <pbommana@google.com>
Cr-Commit-Position: refs/branch-heads/4896@{#382}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify] https://crrev.com/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec/extensions/browser/script_executor.cc
[modify] https://crrev.com/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec/chrome/browser/extensions/api/scripting/scripting_apitest.cc
[add] https://crrev.com/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec/chrome/test/data/extensions/api_test/scripting/nested_web_contents/worker.js
[modify] https://crrev.com/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec/chrome/browser/extensions/api/web_navigation/web_navigation_api.cc
[add] https://crrev.com/382ed1260b5eb60a8bfe9847ce6d2095f2f544ec/chrome/test/data/extensions/api_test/scripting/nested_web_contents/manifest.json

Comment 21 by sheriffbot on Tue, Mar 8, 2022, 1:20 PM EST 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 22 by rzanoni@google.com on Wed, Mar 9, 2022, 7:37 AM EST Project Member

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

Comment 23 by rzanoni@google.com on Wed, Mar 9, 2022, 11:26 AM EST Project Member

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

Comment 24 by sheriffbot on Wed, Mar 9, 2022, 11:30 AM EST 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 25 by gmpritchard@google.com on Wed, Mar 9, 2022, 1:19 PM EST Project Member

Labels: -LTS-Merge-Candidate

Comment 26 by amyressler@chromium.org on Wed, Mar 9, 2022, 5:23 PM EST Project Member

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

M99 merge approved, please merge to branch 4844 NLT 10am PST tomorrow, Thursday, 10 March so this fix can be included in the next stable security refresh being cut tomorrow

M98 merge approved, please merge to branch 4758 so this fix can be included in Extended Stable support

Comment 27 by Git Watcher on Wed, Mar 9, 2022, 7:46 PM EST Project Member

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845

commit f248f0755b5c2a7aa65c45aa33bb54bc69ad3845
Author: Dave Tapuska <dtapuska@chromium.org>
Date: Thu Mar 10 00:45:56 2022

[M99] Do not expose inner WebContents on scripting/getAllFrames.

Inner WebContents shouldn't be exposed for executeScript or getAllFrames
APIs. This is consistent with the API before crrev.com/f894f106
and crrev.com/c8de3b0a.

~~BUG=1301320~~,1261261

(cherry picked from commit 5c4e043324b3afd1be673ae2c0a5c00845bb0e86)

Change-Id: I86a5b09aa44c48319b7dd0a10e5442b8c803d4e5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Dave Tapuska <dtapuska@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977769}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3515013
Cr-Commit-Position: refs/branch-heads/4844@{#1022}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify] https://crrev.com/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845/extensions/browser/script_executor.cc
[modify]
https://crrev.com/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845/chrome/browser/extensions/api/scripting/scripting_apitest.cc
[add]
https://crrev.com/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845/chrome/test/data/extensions/api_test/scripting/nested_web_contents/worker.js
[modify]
https://crrev.com/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845/chrome/browser/extensions/api/web_navigation/web_navigation_api.cc
[add]
https://crrev.com/f248f0755b5c2a7aa65c45aa33bb54bc69ad3845/chrome/test/data/extensions/api_test/scripting/nested_web_contents/manifest.json

Comment 28 by Git Watcher on Wed, Mar 9, 2022, 9:36 PM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b321ac924772586a874927cce2b04600efdf4d69

commit b321ac924772586a874927cce2b04600efdf4d69
Author: Dave Tapuska <dtapuska@chromium.org>
Date: Thu Mar 10 02:35:27 2022

[M98] Do not expose inner WebContents on scripting/getAllFrames.

Inner WebContents shouldn't be exposed for executeScript or getAllFrames
APIs. This is consistent with the API before crrev.com/f894f106
and crrev.com/c8de3b0a.

~~BUG=1301320~~,1261261

(cherry picked from commit 5c4e043324b3afd1be673ae2c0a5c00845bb0e86)

Change-Id: I86a5b09aa44c48319b7dd0a10e5442b8c803d4e5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565
Reviewed-by: Devlin Cronin <rdevlin.cronin@chromium.org>
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Dave Tapuska <dtapuska@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977769}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3514993
Cr-Commit-Position: refs/branch-heads/4758@{#1244}

Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify] https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/extensions/browser/script_executor.cc

[modify] https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/extensions/browser/script_executor.cc
[modify]
https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/chrome/browser/extensions/api/scripting/scripting_apitest.cc
[add]
https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/chrome/test/data/extensions/api_test/scripting/nested_web_contents/worker.js
[modify]
https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/chrome/browser/extensions/api/web_navigation/web_navigation_api.cc
[add]
https://crrev.com/b321ac924772586a874927cce2b04600efdf4d69/chrome/test/data/extensions/api_test/scripting/nested_web_contents/manifest.json

Comment 29 by rzanoni@google.com on Thu, Mar 10, 2022, 3:32 AM EST Project Member

1. Just https://crrev.com/c/3513173
2. Low, simple conflicts on frame iteration loop
3. 98, 99, 100
4. Yes

Comment 30 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:24 PM EST Project Member

Labels: Release-1-M99

Comment 31 by amyressler@chromium.org on Mon, Mar 14, 2022, 12:21 PM EDT Project Member

Labels: -Security_Severity-Critical Security_Severity-High

While this is a UAF in the browser process, it does require a malicious extension to execute, so downgrading to high severity

Comment 32 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0972 CVE_description-missing

Comment 33 by gmpritchard@google.com on Tue, Mar 15, 2022, 9:52 AM EDT Project Member

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

Comment 34 by sheriffbot on Wed, Mar 16, 2022, 1:07 PM EDT Project Member

Labels: -Pri-0 Pri-1

Setting Pri-1 to match security severity High. 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 35 by Git Watcher on Thu, Mar 17, 2022, 6:20 AM EDT Project Member

Labels: merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd

commit 80e73e605d32e57ae6020ec6fe03d07f9d3fffbd
Author: Dave Tapuska <dtapuska@chromium.org>

Author: Dave Tapuska <dtapuska@chromium.org>
Date: Thu Mar 17 10:19:43 2022

[M96-LTS] Do not expose inner WebContents on scripting/getAllFrames.

M96 merge issues:
web_navigation_api.cc:
- M96 uses web_contents->ForEachFrame to iterate the frames while
main uses ForEachRenderFrameHost

Inner WebContents shouldn't be exposed for executeScript or getAllFrames
APIs. This is consistent with the API before crrev.com/f894f106
and crrev.com/c8de3b0a.

~~BUG=1301320~~,1261261

(cherry picked from commit 5c4e043324b3afd1be673ae2c0a5c00845bb0e86)

Change-Id: I86a5b09aa44c48319b7dd0a10e5442b8c803d4e5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497565
Commit-Queue: Dave Tapuska <dtapuska@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977769}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3513173
Reviewed-by: Dave Tapuska <dtapuska@chromium.org>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1535}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd/extensions/browser/script_executor.cc
[modify]
https://crrev.com/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd/chrome/browser/extensions/api/scripting/scripting_apitest.cc
[add]
https://crrev.com/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd/chrome/test/data/extensions/api_test/scripting/nested_web_contents/worker.js
[modify]
https://crrev.com/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd/chrome/browser/extensions/api/web_navigation/web_navigation_api.cc
[add]
https://crrev.com/80e73e605d32e57ae6020ec6fe03d07f9d3fffbd/chrome/test/data/extensions/api_test/scripting/nested_web_contents/manifest.json

Comment 36 by rzanoni@google.com on Thu, Mar 17, 2022, 6:29 AM EDT Project Member

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

Comment 37 by sheriffbot on Sat, Jun 11, 2022, 1:30 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

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

Comment 38 by lukasza@chromium.org on Thu, Jun 30, 2022, 10:47 AM EDT Project Member

Cc: haraken@chromium.org bartekn@chromium.org

Comment 39 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 40 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:14 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing