Starred by 1 user

Owner:	delph...@chromium.org
CC:	sheriffbot mslekova@chromium.org ishell@chromium.org vahl@chromium.org ecmziegler@google.com
Status:	Fixed *(Closed)*
Components:	Blink>JavaScript
Modified:	May 24, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

reward-500
Security_Impact-Stable
Security_Severity-Medium
Hotlist-Merge-Approved
M-80
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-81
merge-merged-8.1
Release-0-M81
CVE-2020-6434
merge-merged-8.3

Issue 1048555: Use after free in CodeSerializer::Deserialize

Reported by gksgu...@gmail.com on Tue, Feb 4, 2020, 3:19 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36

Steps to reproduce the problem:

What is the expected behavior?

What went wrong?
In `CodeSerializer::Deserialize`, `info` is not protected by Handle. And it is used after `SharedFunctionInfo::EnsureSourcePositionsAvailable` triggers a GC, which moves `info` .

```
MaybeHandle<SharedFunctionInfo> CodeSerializer::Deserialize(
    Isolate* isolate, ScriptData* cached_data, Handle<String> source,
    ScriptOriginOptions origin_options) {
  ...
  for (SharedFunctionInfo info = iter.Next(); !info.is_null(); <-- define a raw pointer, `info`
          info = iter.Next()) {
        if (info.is_compiled()) {
          Handle<SharedFunctionInfo> shared_info(info, isolate);
          if (needs_source_positions) {
            SharedFunctionInfo::EnsureSourcePositionsAvailable(isolate,
                                                shared_info); <-- this may call a GC
          }
          DisallowHeapAllocation no_gc;
          int line_num =
              script->GetLineNumber(shared_info->StartPosition()) + 1;
          int column_num =
              script->GetColumnNumber(shared_info->StartPosition()) + 1;
          PROFILE(isolate,
                  CodeCreateEvent(CodeEventListener::SCRIPT_TAG,
                                  handle(info.abstract_code(), isolate), <-- `info` is used.
                                  shared_info, name, line_num, column_num));
        }
      }
  ...
}
```

Patch: Use `shared_info` which is protected by Handle, instead of `info`.

```
MaybeHandle<SharedFunctionInfo> CodeSerializer::Deserialize(
    Isolate* isolate, ScriptData* cached_data, Handle<String> source,
    ScriptOriginOptions origin_options) {
  ...
  for (SharedFunctionInfo info = iter.Next(); !info.is_null();
          info = iter.Next()) {
```

```
      if (info.is_compiled()) {
        Handle<SharedFunctionInfo> shared_info(info, isolate);
        if (needs_source_positions) {
          SharedFunctionInfo::EnsureSourcePositionsAvailable(isolate,
                                                             shared_info);
        }
        DisallowHeapAllocation no_gc;
        int line_num =
            script->GetLineNumber(shared_info->StartPosition()) + 1;
        int column_num =
            script->GetColumnNumber(shared_info->StartPosition()) + 1;
        PROFILE(isolate,
                CodeCreateEvent(CodeEventListener::SCRIPT_TAG,
                                handle(shared_info->abstract_code(), isolate), <-- Use `shared_info` instead of `info`.
                                shared_info, name, line_num, column_num));
      }
    }
  ...
}
```

Did this work before? N/A

Chrome version: 79.0.3945.130 Channel: stable
OS Version: OS X 10.15.2
Flash Version:

Comment 1 by carlosil@chromium.org on Tue, Feb 4, 2020, 5:05 PM EST

Components: Blink>JavaScript

Thanks for reporting, do you have a POC that triggers the UaF? Thanks.

Comment 2 by gksgu...@gmail.com on Tue, Feb 4, 2020, 7:28 PM EST

I'm sorry that I don't have POC. But I think we should use `shared_info` instead of `info` to prevent the UaF bug.

Comment 3 by ishell@chromium.org on Wed, Feb 5, 2020, 4:36 AM EST

Status: Assigned (was: Unconfirmed)
Owner: delph...@chromium.org
Cc: ishell@chromium.org

I'm not sure about actual security implications given that it can be triggered only when the profiling is enabled but it's definitely a raw pointer misuse.
Dan, PTAL.

Comment 4 by ishell@chromium.org on Wed, Feb 5, 2020, 4:44 AM EST

Status: Duplicate (was: Assigned)
Mergedinto: v8:9992

GCMole reported this issue here: ~~issue v8:9992~~.

Comment 5 by ishell@chromium.org on Wed, Feb 5, 2020, 4:46 AM EST

Status: Assigned (was: Duplicate)

Comment 6 Deleted

Comment 7 by gksgu...@gmail.com on Wed, Feb 5, 2020, 5:01 AM EST

@ishell
The report in ~~issue v8:9992~~ ("https://bugs.chromium.org/p/v8/issues/attachmentText?aid=422017") seems to be different from this issue.
GCMole reported about `CreateInterpreterDataForDeserializedCode`, but this issue is about `CodeSerializer::Deserialize`.
Do you mean that this issue is related with ~~issue v8:9992~~?

Comment 8 by ishell@chromium.org on Wed, Feb 5, 2020, 5:13 AM EST

Cc: mslekova@chromium.org

True, thanks!

Maya, FYI. Maybe we can tweak GCMole a bit.

Comment 9 by bugdroid on Wed, Feb 5, 2020, 6:16 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/f57e7da439b26cfb16a79d34f9f56e76e5287aa5

commit f57e7da439b26cfb16a79d34f9f56e76e5287aa5
Author: Dan Elphick <delphick@chromium.org>
Date: Wed Feb 05 11:15:58 2020

[snapshot] Fix deref of raw pointer after potential GC

Fixes the one case after calling EnsureSourcePositionsCollected that we
were still using the non-handle version of the SharedFunctionInfo.

~~Bug: chromium:1048555~~
Change-Id: Iefd35fab13623a1f05212c98864be62c37463942
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2037437
Commit-Queue: Dan Elphick <delphick@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Auto-Submit: Dan Elphick <delphick@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#66130}

[modify] https://crrev.com/f57e7da439b26cfb16a79d34f9f56e76e5287aa5/src/snapshot/code-serializer.cc

Comment 10 by mslekova@chromium.org on Wed, Feb 5, 2020, 7:19 AM EST

@ishell: Thanks for pointing out, GCMole should normally have caught all these similar issues in this file. Did any of you check if there are more left?

Comment 11 by gksgu...@gmail.com on Wed, Feb 5, 2020, 8:03 AM EST

In this week, I already reported 8 similar issues which my tool found. You can find them by searching my account with "use after free" keyword.

Comment 12 by mslekova@chromium.org on Wed, Feb 5, 2020, 8:13 AM EST

Thanks for reporting those. I guess I don't have access to the ones I'm not CC'ed on.
@Dan, should we mark this bug as fixed?

Comment 13 by carlosil@chromium.org on Wed, Feb 5, 2020, 5:35 PM EST

Labels: M-80 Security_Impact-Stable

Comment 14 by carlosil@chromium.org on Wed, Feb 5, 2020, 5:36 PM EST

Labels: Security_Severity-High Security_Needs_Attention-Severity

Assigining severity high, can someone on the V8 side confirm that's the case? Thanks

Comment 15 by gksgu...@gmail.com on Wed, Feb 5, 2020, 8:10 PM EST

And I have some points which are not buggy for now, but may be buggy in the future if we use them incorrectly.
We can enforce their safe usage by changing a few lines. Where should I report them?

Comment 16 by mslekova@chromium.org on Thu, Feb 6, 2020, 4:15 AM EST

gksgudtjr456@ if they're not related to this class, please write them down in a separate issue. Thanks!

Comment 17 by delph...@chromium.org on Thu, Feb 6, 2020, 4:59 AM EST

Labels: -Security_Needs_Attention-Severity Security_Severity-Medium

Re: #14, this bug allows a pointer to memory that has moved to be read. This could then result in a crash or further memory corruption in the renderer process.

That said, it requires the user to have started the profiler, which is not a common action, so I think it falls under these two Medium Memory severity bullet points:
* An out-of-bounds read in a renderer process
* Memory corruption in a renderer process that requires specific user interaction, such as dragging an object

Comment 18 by delph...@chromium.org on Thu, Feb 6, 2020, 5:01 AM EST

Labels: Merge-Request-81

Comment 19 by sheriffbot@chromium.org on Thu, Feb 6, 2020, 11:58 AM EST

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 20 by delph...@chromium.org on Mon, Feb 10, 2020, 3:53 AM EST

Labels: Target-81

Comment 21 by sheriffbot on Fri, Feb 14, 2020, 2:11 PM EST

Labels: -Merge-Request-81 Hotlist-Merge-Approved Merge-Approved-81

Your change meets the bar and is auto-approved for M81. Please go ahead and merge the CL to branch 4044 (refs/branch-heads/4044) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 22 by sheriffbot on Fri, Feb 14, 2020, 8:30 PM EST

Status: Fixed (was: Assigned)

Please mark security bugs as fixed as soon as the fix lands, and before requesting merges. This update is based on the merge- labels applied to this issue. Please reopen if this update was incorrect.

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

Comment 23 by sheriffbot on Sat, Feb 15, 2020, 12:25 PM EST

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

Comment 24 by bugdroid on Mon, Feb 17, 2020, 10:55 AM EST

Labels: merge-merged-8.1

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/3c466721964d924500046c04ec067e5da8c3615e

commit 3c466721964d924500046c04ec067e5da8c3615e
Author: Dan Elphick <delphick@chromium.org>
Date: Mon Feb 17 15:50:30 2020

Merged: [snapshot] Fix deref of raw pointer after potential GC

Revision: f57e7da439b26cfb16a79d34f9f56e76e5287aa5

~~BUG=chromium:1048555~~
NOTRY=true
NOPRESUBMIT=true
NOTREECHECKS=true
R=mythria@chromium.org

Change-Id: Ib1ba3ae35a1fd696ab82495521f9a7d83fddca91
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2060498
Reviewed-by: Mythri Alle <mythria@chromium.org>
Cr-Commit-Position: refs/branch-heads/8.1@{#19}
Cr-Branched-From: a4dcd39d521d14c4b1cac020812e44ee04a7f244-refs/heads/8.1.307@{#1}
Cr-Branched-From: f22c213304ec3542df87019aed0909b7dafeaa93-refs/heads/master@{#66031}

[modify] https://crrev.com/3c466721964d924500046c04ec067e5da8c3615e/src/snapshot/code-serializer.cc

Comment 25 by pbommana@google.com on Mon, Feb 17, 2020, 4:01 PM EST

The CI from comment#24 is already part of M81 branch, delphick@ if all required CL's are in M81 can we please make the bug as fixed.

Comment 26 by delph...@chromium.org on Tue, Feb 18, 2020, 4:34 AM EST

It is marked as fixed.

Comment 27 by natashapabrai@google.com on Tue, Feb 18, 2020, 11:14 AM EST

Labels: reward-topanel

Comment 28 by sheriffbot on Tue, Feb 18, 2020, 12:08 PM EST

Cc: sheriffbot

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 29 by delph...@chromium.org on Tue, Feb 18, 2020, 12:11 PM EST

Labels: -Merge-Approved-81

Comment 30 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:00 PM EST

Labels: -reward-topanel reward-unpaid reward-500

*** 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 31 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:04 PM EST

Nice work! The Panel decided to award $500 for this report

Comment 32 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:08 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 33 by adetaylor@google.com on Mon, Mar 9, 2020, 2:09 PM EDT

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Windows

Comment 34 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT

Labels: Release-0-M81

Comment 35 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:31 PM EDT

Labels: CVE-2020-6434 CVE_description-missing

Comment 36 by bugdroid on Thu, Apr 2, 2020, 8:53 AM EDT

Labels: merge-merged-8.3

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/f57e7da439b26cfb16a79d34f9f56e76e5287aa5

commit f57e7da439b26cfb16a79d34f9f56e76e5287aa5
Author: Dan Elphick <delphick@chromium.org>
Date: Wed Feb 05 11:15:58 2020

[snapshot] Fix deref of raw pointer after potential GC

Fixes the one case after calling EnsureSourcePositionsCollected that we
were still using the non-handle version of the SharedFunctionInfo.

~~Bug: chromium:1048555~~
Change-Id: Iefd35fab13623a1f05212c98864be62c37463942
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2037437
Commit-Queue: Dan Elphick <delphick@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Auto-Submit: Dan Elphick <delphick@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#66130}

[modify] https://crrev.com/f57e7da439b26cfb16a79d34f9f56e76e5287aa5/src/snapshot/code-serializer.cc

Comment 37 by bugdroid on Thu, Apr 2, 2020, 9:14 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/f57e7da439b26cfb16a79d34f9f56e76e5287aa5

commit f57e7da439b26cfb16a79d34f9f56e76e5287aa5
Author: Dan Elphick <delphick@chromium.org>
Date: Wed Feb 05 11:15:58 2020

[snapshot] Fix deref of raw pointer after potential GC

Fixes the one case after calling EnsureSourcePositionsCollected that we
were still using the non-handle version of the SharedFunctionInfo.

~~Bug: chromium:1048555~~
Change-Id: Iefd35fab13623a1f05212c98864be62c37463942
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2037437
Commit-Queue: Dan Elphick <delphick@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Auto-Submit: Dan Elphick <delphick@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#66130}

[modify] https://crrev.com/f57e7da439b26cfb16a79d34f9f56e76e5287aa5/src/snapshot/code-serializer.cc

Comment 38 by bugdroid on Thu, Apr 2, 2020, 9:32 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/f57e7da439b26cfb16a79d34f9f56e76e5287aa5

commit f57e7da439b26cfb16a79d34f9f56e76e5287aa5
Author: Dan Elphick <delphick@chromium.org>
Date: Wed Feb 05 11:15:58 2020

[snapshot] Fix deref of raw pointer after potential GC

Fixes the one case after calling EnsureSourcePositionsCollected that we

were still using the non-handle version of the SharedFunctionInfo.

~~Bug: chromium:1048555~~
Change-Id: Iefd35fab13623a1f05212c98864be62c37463942
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2037437
Commit-Queue: Dan Elphick <delphick@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Auto-Submit: Dan Elphick <delphick@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#66130}

[modify] https://crrev.com/f57e7da439b26cfb16a79d34f9f56e76e5287aa5/src/snapshot/code-serializer.cc

Comment 39 by bugdroid on Thu, Apr 2, 2020, 10:02 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/f57e7da439b26cfb16a79d34f9f56e76e5287aa5

commit f57e7da439b26cfb16a79d34f9f56e76e5287aa5
Author: Dan Elphick <delphick@chromium.org>
Date: Wed Feb 05 11:15:58 2020

[snapshot] Fix deref of raw pointer after potential GC

Fixes the one case after calling EnsureSourcePositionsCollected that we
were still using the non-handle version of the SharedFunctionInfo.

~~Bug: chromium:1048555~~
Change-Id: Iefd35fab13623a1f05212c98864be62c37463942
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2037437
Commit-Queue: Dan Elphick <delphick@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Auto-Submit: Dan Elphick <delphick@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/master@{#66130}

[modify] https://crrev.com/f57e7da439b26cfb16a79d34f9f56e76e5287aa5/src/snapshot/code-serializer.cc

Comment 40 by adetaylor@chromium.org on Tue, Apr 14, 2020, 3:14 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 41 by sheriffbot on Sun, May 24, 2020, 2:54 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