Starred by 6 users

Owner: tebbi@chromium.org

CC: mache...@chromium.org
rzanoni@google.com
billyleonard@google.com
leszeks@chromium.org
saelo@google.com
weihengchen@google.com
tebbi@chromium.org
ecmziegler@chromium.org
adetaylor@google.com
verwa...@chromium.org
amyressler@chromium.org
thibaudm@chromium.org
clemensb@chromium.org
shuntley@google.com
noelutz@google.com
vahl@chromium.org
ecmziegler@google.com

Status: Verified *(Closed)*

Components: Blink>JavaScript>Compiler>Turbofan

Modified: Aug 22, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac

Pri: 0

Type: Bug-Security

M-100
Security_Severity-High
ReleaseBlock-Stable
allpublic
ClusterFuzz-Verified
Test-Predator-Auto-Owner
CVE_description-submitted
Target-100
FoundIn-100
FoundIn-101

FoundIn-102
M-101
Target-101

Issue 1315901: Security: [0-day] JIT optimisation issue

Reported by cleci...@google.com on Wed, Apr 13, 2022, 5:03 AM EDT Project Member

Code

NOTE: We have evidence that the following bug is being used in the wild. Therefore, this bug is subject to a 7 day disclosure deadline.

VULNERABILITY DETAILS

Seems to be a JIT optimisation issue in Turbofan (confirmed by saelo@) but we don't have a full root cause analysis. Filling this bug now as it is used in the wild and we have a poc triggering the issue.

VERSION
Chrome Version: 100.0.4896.79 + HEAD

REPRODUCTION CASE

```
function foo(bug) {
  function C(z) {
    Error.prepareStackTrace = function(t, B) {
      return B[z].getThis();
    };
    let p = Error().stack;
    Error.prepareStackTrace = null;
    return p;
  }
  function J() {}
  var optim = false;
  var opt = new Function(
      'a', 'b', 'c',
      'if(typeof a===\'number\'){if(a>2){for(var i=0;i<100;i++);return;}b.d(a,b,1);return}' +
          'g++;'.repeat(70));
  var e = null;
  J.prototype.d = new Function(
      'a', 'b', '"use strict";b.a.call(arguments,b);return arguments[a];');
  J.prototype.a = new Function('a', 'a.b(0,a)');
  J.prototype.b = new Function(
      'a', 'b',
      'b.c();if(a){' +
          'g++;'.repeat(70) + '}');
  J.prototype.c = function() {
    if (optim) {
      var z = C(3);
      var p = C(3);
      z[0] = 0;
      e = {M: z, C: p};
    }
  };
  var a = new J();
```

```
  // jit optim
  if (bug) {
    for (var V = 0; 1E4 > V; V++) {
      opt(0 == V % 4 ? 1 : 4, a, 1);
    }
  }
  optim = true;
  opt(1, a, 1);
  return e;
}

e1 = foo(false);
console.log(e1.M === e1.C); // prints true.
e2 = foo(true);
console.log(e2.M === e2.C); // should be true as above but prints false.
```

CREDIT INFORMATION
Clément Lecigne of Google's Threat Analysis Group

poc.js
1.1 KB View Download

Comment 1 by saelo@google.com on Wed, Apr 13, 2022, 5:08 AM EDT Project Member

Cc: thibaudm@chromium.org clemensb@chromium.org tebbi@chromium.org ecmziegler@chromium.org adetaylor@google.com
Components: Blink>JavaScript>Compiler>Turbofan

Taking a closer look at the trigger now. The sample does print `true true` if run with `--no-opt`, so it's likely a turbofan issue.

Comment 2 by saelo@google.com on Wed, Apr 13, 2022, 5:55 AM EDT Project Member

What seems to be happening here is that the code somehow ends up creating two different JSArgumentsObjects (`e2.M` and `e2.C`) which point to the same `FixedArray` elements backing store. This can be seen by adding `%DebugPrint` statements at the end of the repro case:

```
========== e2.M ==========

DebugPrint: 0x85700257e05: [JS_ARGUMENTS_OBJECT_TYPE] in OldSpace
  ...
 - elements: 0x0857000d9a49 <FixedArray[3]>

...

========== e2.C ==========

DebugPrint: 0x85700257e35: [JS_ARGUMENTS_OBJECT_TYPE] in OldSpace
  ...
 - elements: 0x0857000d9a49 <FixedArray[3]>

...
```

```

It seems this can then be used to cause other issues. For example, by deleting e.g. `e2.M[0]` then accessing `e2.C[0]` you can leak the "hole" value, which can probably be used to cause memory corruption (see e.g. ~~issue 1263462~~).

Comment 3 by cleci...@google.com on Wed, Apr 13, 2022, 6:59 AM EDT Project Member

**Cc:** noelutz@google.com

Comment 4 by saelo@google.com on Wed, Apr 13, 2022, 7:31 AM EDT Project Member

**Labels:** Pri-0

Comment 5 by ClusterFuzz on Wed, Apr 13, 2022, 8:11 AM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5432723191824384.

Comment 6 by saelo@google.com on Wed, Apr 13, 2022, 8:20 AM EDT Project Member

The testcase uploaded to clusterfuzz half-exploits the bug (relevant code copied from ~~issue 1263462~~) to force a crash in both debug and release builds by leaking the hole value and using it to create a corrupted JSMap object.

Comment 7 by ClusterFuzz on Wed, Apr 13, 2022, 8:29 AM EDT Project Member

**Labels:** OS-Mac OS-Linux

Comment 8 by ClusterFuzz on Wed, Apr 13, 2022, 8:47 AM EDT Project Member

**Status:** Assigned (was: Unconfirmed)
**Owner:** emrich@google.com
**Labels:** Test-Predator-Auto-Owner

Automatically assigning owner based on suspected regression changelist https://chromium.googlesource.com/v8/v8/+/b4fe3473e4c9e6adc2d7439876e6752c45cdff04 ([dict-proto] make ordered hash tables use InternalIndex for indices).

If this is incorrect, please let us know why and apply the Test-Predator-Wrong-CLs label. If you aren't the correct owner for this issue, please unassign yourself as soon as possible so it can be re-triaged.

Comment 9 by saelo@google.com on Wed, Apr 13, 2022, 9:00 AM EDT Project Member

**Owner:** tebbi@chromium.org
**Labels:** Security_Severity-High FoundIn-100

The bisected CL is probably just the one that made this way of exploiting the "hole" possible, not the one actually introducing the bug. Reassigning to tebbi@ who has more knowledge of Turbofan and the escape analysis pass (to which this bugs seems to be related) for now, but feel free to reassign!

Comment 10 by sheriffbot on Wed, Apr 13, 2022, 9:04 AM EDT Project Member

**Labels:** Security_Impact-Extended

Comment 11 by ClusterFuzz on Wed, Apr 13, 2022, 9:07 AM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6447647451578368.
```

Comment 12 by ClusterFuzz on Wed, Apr 13, 2022, 9:34 AM EDT Project Member

Labels: FoundIn-101 FoundIn-102

Detailed Report: https://clusterfuzz.com/testcase?key=6447647451578368

Fuzzer: None
Job Type: linux_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
!value->IsTheHole(isolate) in objects.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=49094:49095

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=6447647451578368

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 13 by saelo@google.com on Wed, Apr 13, 2022, 10:24 AM EDT Project Member

Cc: verwa...@chromium.org leszeks@chromium.org

Comment 14 by amyressler@chromium.org on Wed, Apr 13, 2022, 11:03 AM EDT Project Member

Cc: amyressler@chromium.org

Comment 15 by ClusterFuzz on Wed, Apr 13, 2022, 12:19 PM EDT Project Member

Detailed Report: https://clusterfuzz.com/testcase?key=5432723191824384

Fuzzer: None
Job Type: linux_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
table->NumberOfDeletedElements() == removed_holes_index in ordered-hash-table.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=70872:70873

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5432723191824384

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 16 by sheriffbot on Wed, Apr 13, 2022, 12:47 PM EDT Project Member

Labels: M-100 Target-100

Setting milestone and target because of high severity.

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

Comment 17 by gov...@chromium.org on Wed, Apr 13, 2022, 12:57 PM EDT Project Member

Labels: OS-Android OS-Windows

Comment 18 by gov...@chromium.org on Wed, Apr 13, 2022, 1:04 PM EDT Project Member

Labels: ReleaseBlock-Stable M-101 Target-101

Comment 19 by sheriffbot on Wed, Apr 13, 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 20 by Git Watcher on Wed, Apr 13, 2022, 1:31 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940

commit 8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Apr 13 16:30:36 2022

[compiler] mark receiver and function as escaping

~~Bug: chromium:1315901~~
Change-Id: Ic44bfcae32aba202ba25c5f59fe579214a444584
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3584117
Reviewed-by: Leszek Swirski <leszeks@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79968}

[modify] https://crrev.com/8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940/src/compiler/escape-analysis.cc

Comment 21 by Git Watcher on Wed, Apr 13, 2022, 1:37 PM EDT Project Member

Labels: merge-merged-5002

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/1da81b4637cdb4d16bb7c13c5160a4e57debfe9c

commit 1da81b4637cdb4d16bb7c13c5160a4e57debfe9c
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Apr 13 16:30:36 2022

[compiler] mark receiver and function as escaping

~~Bug: chromium:1315901~~
Change-Id: Ic44bfcae32aba202ba25c5f59fe579214a444584
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3584117
Reviewed-by: Leszek Swirski <leszeks@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79968}
(cherry picked from commit 8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940)
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3585782
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>

[modify] https://crrev.com/1da81b4637cdb4d16bb7c13c5160a4e57debfe9c/src/compiler/escape-analysis.cc

Comment 22 by amyressler@chromium.org on Wed, Apr 13, 2022, 2:00 PM EDT Project Member

Status: Fixed (was: Assigned)
Labels: Merge-Request-100 Merge-Request-101

hi tebbi@, thank you so much for the quick fix and merge for Canary.
Following up with coordinating with the Release Team, please prepare a merge to the V8 release branch for M100 (10.0-lkgr), we would like this to get merged as soon as possible so we can ensure the mini branch for the emergency release is picked up. Thanks!

Comment 23 by sheriffbot on Wed, Apr 13, 2022, 2:00 PM 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 24 by Git Watcher on Wed, Apr 13, 2022, 2:34 PM EDT Project Member

Labels: merge-merged-10.0

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/2c8d797fee04bc385c5a866235a88eb62c39ffb7

commit 2c8d797fee04bc385c5a866235a88eb62c39ffb7
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Apr 13 16:30:36 2022

Merged: [compiler] mark receiver and function as escaping

~~Bug: chromium:1315901~~

(cherry picked from commit 8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940)

Change-Id: I02677d3fd11f5513d5d1235279acc89ded49e762
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3585902
Owners-Override: Tobias Tebbi <tebbi@chromium.org>
Reviewed-by: Dominik Inführ <dinfuehr@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.0@{#28}
Cr-Branched-From: 6ea73a738c467dc26abbbe84e27a36aac1c6e119-refs/heads/10.0.139@{#1}
Cr-Branched-From: ccc689011280419901e6ee42cae39980c0e96030-refs/heads/main@{#79131}

[modify] https://crrev.com/2c8d797fee04bc385c5a866235a88eb62c39ffb7/src/compiler/escape-analysis.cc

Comment 25 by Git Watcher on Wed, Apr 13, 2022, 2:35 PM EDT Project Member

Labels: merge-merged-10.1

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/bc8f9a2d23d4622637fdb6d6095bf2061302e983

commit bc8f9a2d23d4622637fdb6d6095bf2061302e983
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Apr 13 16:30:36 2022

[compiler] mark receiver and function as escaping

~~Bug: chromium:1315901~~

(cherry picked from commit 8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940)

Change-Id: I17eee86e6d5284c64a19ee019cb3df38a71b4cf8
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3585903
Reviewed-by: Dominik Inführ <dinfuehr@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.1@{#20}
Cr-Branched-From: b003970395b7efcc309eb30b4ca06dd8385acd55-refs/heads/10.1.124@{#1}
Cr-Branched-From: e62f556862624103ea1da5b9dcef9b216832033b-refs/heads/main@{#79503}

[modify] https://crrev.com/bc8f9a2d23d4622637fdb6d6095bf2061302e983/src/compiler/escape-analysis.cc

Comment 26 by gmpritchard@google.com on Wed, Apr 13, 2022, 2:52 PM EDT Project Member

Can someone please confirm if this needs to be merged to 9.6 (LTS) as well?

Comment 27 by rzanoni@google.com on Wed, Apr 13, 2022, 3:04 PM EDT Project Member

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

Comment 28 by amyressler@chromium.org on Wed, Apr 13, 2022, 4:17 PM EDT Project Member

Labels: Pri-0

Comment 29 by tebbi@chromium.org on Wed, Apr 13, 2022, 4:25 PM EDT Project Member

The bug is around since at least 2017, so pretty sure this also affects 9.6 LTS.

Comment 30 by ClusterFuzz on Wed, Apr 13, 2022, 4:35 PM EDT Project Member

Detailed Report: https://clusterfuzz.com/testcase?key=5432723191824384

Fuzzer: None
Job Type: linux_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
table->NumberOfDeletedElements() == removed_holes_index in ordered-hash-table.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=70872:70873
Fixed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=79967:79968

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5432723191824384

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 31 by gov...@chromium.org on Wed, Apr 13, 2022, 6:55 PM EDT Project Member

Labels: -Merge-Request-100 -Merge-Request-101 merge-merged-100 merge-merged-101

Already merged to M100 and M101 at #24 and #25.

Comment 32 by sheriffbot on Thu, Apr 14, 2022, 3:35 AM EDT Project Member

Labels: V8-postmortem

This high+ V8 security issue with stable impact requires a lightweight post mortem. Please take some time to answer questions asked in this form [1] to help us improve V8 security. [1] https://docs.google.com/forms/d/e/1FAIpQLSdSMCiEpIFLLFkMbgtulK1sf1B-idQmkFaA4XP2Rz5mN1cqWg/viewform?usp=pp_url&entry.307501673=1315901&entry.364066060=Internal&entry.958145677=Android&entry.958145677=Chrome&entry.958145677=Linux&entry.958145677=Mac&entry.958145677=Windows&entry.763880440=Extended&entry.1678852700=High&entry.763402679=Blink>JavaScript>Compiler>Turbofan&entry.975983575=tebbi@chromium.org Please ensure to copy the full link, as otherwise some issue meta data might not be populated automatically.

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

Comment 33 by vahl@chromium.org on Thu, Apr 14, 2022, 4:12 AM EDT Project Member

No need to merge to M102 either as the patch landed before the V8 10.2 branch was created https://chromium.googlesource.com/v8/v8/+log/refs/heads/10.2-lkgr inclused the fix

Comment 34 by tebbi@chromium.org on Thu, Apr 14, 2022, 4:25 AM EDT Project Member

It might be possible to circumvent yesterday's patch (kudos to saelo@ for spotting this). If it's possible, it's probably quite some work to get it working, because it requires applying `.getThis` on an inlined builtin continuation frame (like Array.prototype.forEach), so for example it can't be an arguments object anymore.

In any case, I prepared an improved patch that should land in V8 within half an hour (https://chromium-review.googlesource.com/c/v8/v8/+/3585948).

Comment 35 by tebbi@chromium.org on Thu, Apr 14, 2022, 4:27 AM EDT Project Member

How should we proceed with the expanded patch regarding back-merges and releases?

Comment 36 by Git Watcher on Thu, Apr 14, 2022, 4:45 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/b32605ee8d5137024d335e0fa2a5c0a2529f7881

commit b32605ee8d5137024d335e0fa2a5c0a2529f7881
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Thu Apr 14 07:57:08 2022

[compiler] mark receiver and function as escaping, expanded to continuation frames

~~Bug: chromium:1315901~~
Change-Id: I99ed1562356676f54e69a832c8e862c1cf74fb07
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3585948
Reviewed-by: Samuel Groß <saelo@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79984}

[modify] https://crrev.com/b32605ee8d5137024d335e0fa2a5c0a2529f7881/src/compiler/escape-analysis.cc

Comment 37 by saelo@google.com on Thu, Apr 14, 2022, 5:36 AM EDT Project Member

Our current assessment is that the bug is no longer exploitable when only the first patch is applied. However, without the 2nd patch, a variant of the bug still exists, and can be triggered with fairly small modifications, but seemingly can no longer be exploited: while the broken objects are still created by the engine, they aren't exposed to the user script, so can't be abused to leak the hole or similar things.
However, even if the 2nd patch may not be strictly necessary, we'd definitely be in favor of also back-merging that patch to be on the safe side.

Comment 38 by rzanoni@google.com on Thu, Apr 14, 2022, 8:32 AM EDT Project Member

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

Comment 39 by sheriffbot on Thu, Apr 14, 2022, 8:36 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 40 by rzanoni@google.com on Thu, Apr 14, 2022, 8:42 AM EDT Project Member

1. Just https://crrev.com/c/3584531
2. Low, no conflicts
3. Merged to main on Apr 13
4. Yes

Comment 41 by gmpritchard@google.com on Thu, Apr 14, 2022, 11:13 AM EDT Project Member

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

@rzanoni let's wait until it gets pushed in Stable. I'll approve right after that.

Comment 42 by amyressler@chromium.org on Thu, Apr 14, 2022, 11:27 AM EDT Project Member

Thank you saelo@ for the finding (+verwaest@ and tebbi@ that helped lead to the analysis for the fix) && tebbi@ for the quick landing of the second patch.

Given that the original issue is being actively exploited ITW, the current plan is to release the original fix in an emergency release today (since it has been merged and can be released today as per the original plan) as the risk of leaving this unpatched longer seems much higher than waiting for the new patch as per comment #37 and in our off-bug discussion.

In parallel, the new patch (comment #36) can be allowed sufficient bake time on Canary and then backmerged to M100 and M101 next week to go out in the next releases of each.

Comment 43 by ClusterFuzz on Thu, Apr 14, 2022, 11:55 AM EDT Project Member

Status: Verified (was: Fixed)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 6447647451578368 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=79967:79968

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 44 by amyressler@chromium.org on Thu, Apr 14, 2022, 1:36 PM EDT Project Member

Labels: Release-3-M100

Comment 45 by amyressler@google.com on Thu, Apr 14, 2022, 1:45 PM EDT Project Member

Labels: CVE-2022-1364 CVE_description-missing

Comment 46 by adetaylor@google.com on Fri, Apr 15, 2022, 1:16 PM EDT Project Member

Cc: weihengchen@google.com

Comment 47 by gmpritchard@google.com on Fri, Apr 15, 2022, 1:29 PM EDT Project Member

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

Comment 48 by sheriffbot on Fri, Apr 15, 2022, 1:40 PM EDT Project Member

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

Comment 49 by Git Watcher on Mon, Apr 18, 2022, 9:57 AM EDT Project Member

Labels: merge-merged-9.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/b2d3ef69ef992d2dc2f1733e3c17c361357516dd

commit b2d3ef69ef992d2dc2f1733e3c17c361357516dd
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Apr 13 16:30:36 2022

[M96-LTS][compiler] mark receiver and function as escaping

(cherry picked from commit 8081a5ffa7ebdb0e5b35cf63aa0490ad3578b940)

~~Bug: chromium:1315901~~
No-Try: true
No-Presubmit: true
No-Tree-Checks: true
Change-Id: Ic44bfcae32aba202ba25c5f59fe579214a444584
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3584117
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#79968}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3584531
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Reviewed-by: Nico Hartmann <nicohartmann@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/9.6@{#62}
Cr-Branched-From: 0b7bda016178bf438f09b3c93da572ae3663a1f7-refs/heads/9.6.180@{#1}
Cr-Branched-From: 41a5a247d9430b953e38631e88d17790306f7a4c-refs/heads/main@{#77244}

[modify] https://crrev.com/b2d3ef69ef992d2dc2f1733e3c17c361357516dd/src/compiler/escape-analysis.cc

Comment 50 by rzanoni@google.com on Mon, Apr 18, 2022, 9:58 AM EDT Project Member

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

Comment 51 by amyressler@chromium.org on Mon, Apr 18, 2022, 9:03 PM EDT Project Member

hi tebbi@ -- rather than adding new merge labels, I just wanted to check in that the secondary patch got/gets merged to M101 and M100 now that it had super sufficient bake time in Canary over the long weekend in the EU. I don't believe this has been achieved just yet, so could you please merge the secondary patch to 10.1-lkgr and 10.0-lkgr ASAP so that patch can be included in the Tuesday PDT release cut for M101 Stable and M100 Extended -- thank you!

Comment 52 by Git Watcher on Tue, Apr 19, 2022, 3:16 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/5bfe521a1c4165ae7afae68c32e105e945e6af35

commit 5bfe521a1c4165ae7afae68c32e105e945e6af35
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Thu Apr 14 07:57:08 2022

Merged: [compiler] mark receiver and function as escaping, expanded to continuation frames

~~Bug: chromium:1315901~~

(cherry picked from commit b32605ee8d5137024d335e0fa2a5c0a2529f7881)

Change-Id: I3009b7d1e7dc6c215d6c4b1ccb03f30aa276e847
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3591333
Reviewed-by: Lutz Vahl <vahl@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.1@{#22}
Cr-Branched-From: b003970395b7efcc309eb30b4ca06dd8385acd55-refs/heads/10.1.124@{#1}
Cr-Branched-From: e62f556862624103ea1da5b9dcef9b216832033b-refs/heads/main@{#79503}

[modify] https://crrev.com/5bfe521a1c4165ae7afae68c32e105e945e6af35/src/compiler/escape-analysis.cc

Comment 53 by Git Watcher on Tue, Apr 19, 2022, 3:17 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/1b752a59e5d37ba51ec2b89fb193b0339b1bcae3

commit 1b752a59e5d37ba51ec2b89fb193b0339b1bcae3
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Thu Apr 14 07:57:08 2022

Merged: [compiler] mark receiver and function as escaping, expanded to continuation frames

~~Bug: chromium:1315901~~

(cherry picked from commit b32605ee8d5137024d335e0fa2a5c0a2529f7881)

Change-Id: If37786578e47e31acc4ccf40bb82175c3ee038cc
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3592754
Reviewed-by: Lutz Vahl <vahl@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.0@{#30}
Cr-Branched-From: 6ea73a738c467dc26abbbe84e27a36aac1c6e119-refs/heads/10.0.139@{#1}
Cr-Branched-From: ccc689011280419901e6ee42cae39980c0e96030-refs/heads/main@{#79131}

[modify] https://crrev.com/1b752a59e5d37ba51ec2b89fb193b0339b1bcae3/src/compiler/escape-analysis.cc

Comment 54 by gmpritchard@google.com on Tue, Apr 19, 2022, 10:24 AM EDT Project Member

Labels: LTS-Merge-Approved-96

Comment 55 by Git Watcher on Wed, Apr 27, 2022, 4:19 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/66c8de2cdac10cad9e622ecededda411b44ac5b3

commit 66c8de2cdac10cad9e622ecededda411b44ac5b3
Author: Samuel Groß <saelo@chromium.org>
Date: Tue Apr 19 12:49:01 2022

Harden Map.prototype.delete and related methods

These can be tricked into corrupting memory when an attacker can leak
the "hole" value due to a bug. This CL simply adds CHECKs to prevent
this. A longer-term solution might be to introduce "special-purpose
holes" so that a leaked "hole" value can no longer be used to confuse
unrelated code like the JSMap implementation because that would then use
a different "hole" value.

~~Bug: chromium:1315901~~
Change-Id: Id6c432d39fb97002fa67efe90d34014fc5408ba3
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3593783
Reviewed-by: Toon Verwaest <verwaest@chromium.org>
Commit-Queue: Samuel Groß <saelo@chromium.org>
Cr-Commit-Position: refs/heads/main@{#80201}

[modify] https://crrev.com/66c8de2cdac10cad9e622ecededda411b44ac5b3/src/builtins/builtins-collections-gen.cc

Comment 56 by rzanoni@google.com on Thu, Apr 28, 2022, 12:41 PM EDT Project Member

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

Labelling as LTS candidate for 96 again because of https://crrev.com/c/3593783 that was recently merged

Comment 57 by rzanoni@google.com on Thu, Apr 28, 2022, 12:51 PM EDT Project Member

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

Comment 58 by sheriffbot on Thu, Apr 28, 2022, 12:56 PM 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 59 by rzanoni@google.com on Thu, Apr 28, 2022, 1:02 PM EDT Project Member

1. Just https://crrev.com/c/3614969
2. Low, no conflicts

3. Merged to main on Apr 27
4. Yes

Comment 60 by saelo@google.com on Fri, Apr 29, 2022, 4:21 AM EDT Project Member

I'm not sure https://crrev.com/c/3593783 needs to be backported since it's only a defense-in-depth hardening measure and not fixing a particular bug.

Comment 61 by rzanoni@google.com on Fri, Apr 29, 2022, 8:57 AM EDT Project Member

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

saelo@ thanks for clarifying, I will abandon the cherry-pick and keep only the merged fix

Comment 62 by mache...@chromium.org on Mon, May 2, 2022, 3:46 AM EDT Project Member

Cc: mache...@chromium.org

Did a regression test land? Tebbi, can you make sure that we have improved test cases for this situation, in particular one regression test for the exact case, which then can be picked up by fuzzers again?

Comment 63 by tebbi@chromium.org on Tue, May 3, 2022, 11:17 AM EDT Project Member

I'll land a regression test as soon as the bug becomes public.

Comment 64 by Git Watcher on Tue, Jun 28, 2022, 10:47 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/add8811019a1f2015c4214c20df8e6e8d4a864bb

commit add8811019a1f2015c4214c20df8e6e8d4a864bb
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Tue Jun 28 10:03:11 2022

[compiler] improve escape analysis for receivers and closures

When a receiver/closure is not used by a lazy deopt frame state, then
it cannot escape through the .getThis API. Therefore, it's safe to
dematerialize it.

~~Bug: chromium:1315901~~, ~~chromium:1318126~~
Change-Id: I5cf9c30e8451a7af94d371162a94eb1ba0c9db4a
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3726299
Reviewed-by: Nico Hartmann <nicohartmann@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Reviewed-by: Jakob Kummerow <jkummerow@chromium.org>
Cr-Commit-Position: refs/heads/main@{#81415}

[modify] https://crrev.com/add8811019a1f2015c4214c20df8e6e8d4a864bb/src/execution/frames.cc
[modify] https://crrev.com/add8811019a1f2015c4214c20df8e6e8d4a864bb/src/compiler/escape-analysis.cc

Comment 65 by tebbi@chromium.org on Wed, Jun 29, 2022, 6:51 AM EDT Project Member

Thanks to a recently added CHECK, Clusterfuzz found (https://bugs.chromium.org/p/chromium/issues/detail?id=1340335) a variant where escape analysis still dematerializes a receiver observable from a stack trace, which is the root cause for this issue. Therefore, it is likely that this issue is still exploitable. I'm landing a fix right now.

Comment 66 by Git Watcher on Wed, Jun 29, 2022, 7:02 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/17da9e70833014e0a2646db5c11588f0aee02de7

commit 17da9e70833014e0a2646db5c11588f0aee02de7
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Jun 29 10:18:59 2022

[compiler] fix FrameState revisit bug in escape analysis

~~Bug: chromium:1340335~~, ~~chromium:1315901~~
Change-Id: Ic348e8a66df098f64cf1893f83c145ac7bdb1ecb
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3732939
Reviewed-by: Maya Lekova <mslekova@chromium.org>
Commit-Queue: Tobias Tebbi <tebbi@chromium.org>
Auto-Submit: Tobias Tebbi <tebbi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#81434}

[modify] https://crrev.com/17da9e70833014e0a2646db5c11588f0aee02de7/src/compiler/escape-analysis.cc

Comment 67 by Git Watcher on Mon, Jul 11, 2022, 6:50 AM EDT Project Member

Labels: merge-merged-10.3

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/104c57e51e909df772eb064dd3098ae41ecb8bbf

commit 104c57e51e909df772eb064dd3098ae41ecb8bbf
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Jun 29 10:18:59 2022

Merged: [compiler] fix FrameState revisit bug in escape analysis

(cherry picked from commit 17da9e70833014e0a2646db5c11588f0aee02de7)

~~Bug: chromium:1340335~~, ~~chromium:1315901~~
Change-Id: I62a90686802f814b3e1f15987f3e42b89a30525b
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3755142
Reviewed-by: Thibaud Michaud <thibaudm@chromium.org>
Commit-Queue: Samuel Groß <saelo@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.3@{#35}
Cr-Branched-From: 1a8f4cab47232e7861928945eeee1c40fe7f7c08-refs/heads/10.3.174@{#1}
Cr-Branched-From: 8fbefa47971832fc5afaffb913ae9689f0cc9f9e-refs/heads/main@{#80471}

[modify] https://crrev.com/104c57e51e909df772eb064dd3098ae41ecb8bbf/src/compiler/escape-analysis.cc

Comment 68 by Git Watcher on Mon, Jul 11, 2022, 6:51 AM EDT Project Member

Labels: merge-merged-10.2

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/8ea66a7833e20844d70f946105d32e5c4384d8e5

commit 8ea66a7833e20844d70f946105d32e5c4384d8e5
Author: Tobias Tebbi <tebbi@chromium.org>

Date: Wed Jun 29 10:18:59 2022

Merged: [compiler] fix FrameState revisit bug in escape analysis

(cherry picked from commit 17da9e70833014e0a2646db5c11588f0aee02de7)

~~Bug: chromium:1340335~~, ~~chromium:1315901~~
Change-Id: I81cdc6bc3d6c7441ebc333d33801329c05fbd5d4
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3755103
Reviewed-by: Thibaud Michaud <thibaudm@chromium.org>
Commit-Queue: Samuel Groß <saelo@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.2@{#25}
Cr-Branched-From: 374091f382e88095694c1283cbdc2acddc1b1417-refs/heads/10.2.154@{#1}
Cr-Branched-From: f0c353f6315eeb2212ba52478983a3b3af07b5b1-refs/heads/main@{#79976}

[modify] https://crrev.com/8ea66a7833e20844d70f946105d32e5c4384d8e5/src/compiler/escape-analysis.cc

Comment 69 by Git Watcher on Mon, Jul 11, 2022, 6:52 AM EDT Project Member

Labels: merge-merged-10.4

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/203af1ba6b7bb000f979eb1d38fd950af8247fe8

commit 203af1ba6b7bb000f979eb1d38fd950af8247fe8
Author: Tobias Tebbi <tebbi@chromium.org>
Date: Wed Jun 29 10:18:59 2022

Merged: [compiler] fix FrameState revisit bug in escape analysis

(cherry picked from commit 17da9e70833014e0a2646db5c11588f0aee02de7)

~~Bug: chromium:1340335~~, ~~chromium:1315901~~
Change-Id: I69b063c531abf714f37549e5a116142ccee15831
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3755102
Commit-Queue: Samuel Groß <saelo@chromium.org>
Reviewed-by: Thibaud Michaud <thibaudm@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.4@{#29}
Cr-Branched-From: b1413ed7c71ababe05d590de4b5c4ed97b68693e-refs/heads/10.4.132@{#1}
Cr-Branched-From: 9d0a09368569234a1d1094975e2e92591922cd08-refs/heads/main@{#80972}

[modify] https://crrev.com/203af1ba6b7bb000f979eb1d38fd950af8247fe8/src/compiler/escape-analysis.cc

Comment 70 by Git Watcher on Mon, Jul 11, 2022, 8:40 AM EDT Project Member

Labels: merge-merged-5112 merge-merged-104

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ac1ef1a1ff9099bb1fde1aa2cc9613f6fcec8101

commit ac1ef1a1ff9099bb1fde1aa2cc9613f6fcec8101
Author: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Date: Mon Jul 11 12:39:52 2022

Roll v8 10.4 from f19d0a673665 to 069429ea4663 (2 revisions)

https://chromium.googlesource.com/v8/v8.git/+log/f19d0a673665..069429ea4663

2022-07-11 v8-ci-autoroll-builder@chops-service-accounts.iam.gserviceaccount.com Version 10.4.132.17
2022-07-11 tebbi@chromium.org Merged: [compiler] fix FrameState revisit bug in escape analysis

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/v8-chromium-release-0
Please CC v8-waterfall-sheriff@grotations.appspotmail.com on the revert to ensure that a human
is aware of the problem.

To file a bug in v8 10.4: https://bugs.chromium.org/p/v8/issues/entry
To file a bug in Chromium m104: https://bugs.chromium.org/p/chromium/issues/entry

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+doc/main/autoroll/README.md

~~Bug: chromium:1315901~~,~~chromium:1340335~~
Tbr: v8-waterfall-sheriff@grotations.appspotmail.com
Change-Id: I3a07c4df034da49ea6f89d727280ed7503ac2ca0
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3755581
Bot-Commit: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Commit-Queue: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/5112@{#765}
Cr-Branched-From: b13d3fe7b3c47a56354ef54b221008afa754412e-refs/heads/main@{#1012729}

[modify] https://crrev.com/ac1ef1a1ff9099bb1fde1aa2cc9613f6fcec8101/DEPS

Comment 71 by Git Watcher on Mon, Jul 11, 2022, 8:51 AM EDT Project Member

Labels: merge-merged-5060 merge-merged-103

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d6df80c470aea2127368ad2d4e047a4a197b5619

commit d6df80c470aea2127368ad2d4e047a4a197b5619
Author: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Date: Mon Jul 11 12:50:34 2022

Roll v8 10.3 from 9612bf8fb900 to 9abdc4cc595e (2 revisions)

https://chromium.googlesource.com/v8/v8.git/+log/9612bf8fb900..9abdc4cc595e

2022-07-11 v8-ci-autoroll-builder@chops-service-accounts.iam.gserviceaccount.com Version 10.3.174.20
2022-07-11 tebbi@chromium.org Merged: [compiler] fix FrameState revisit bug in escape analysis

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/v8-chromium-release-1
Please CC v8-waterfall-sheriff@grotations.appspotmail.com on the revert to ensure that a human

is aware of the problem.

To file a bug in v8 10.3: https://bugs.chromium.org/p/v8/issues/entry
To file a bug in Chromium m103: https://bugs.chromium.org/p/chromium/issues/entry

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+doc/main/autoroll/README.md

~~Bug: chromium:1315901~~,~~chromium:1340335~~
Tbr: v8-waterfall-sheriff@grotations.appspotmail.com
Change-Id: I31011939ea3d94a51ff495fd8c90a9318cdae610
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3753434
Bot-Commit: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Commit-Queue: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/5060@{#1192}
Cr-Branched-From: b83393d0f4038aeaf67f970a024d8101df7348d1-refs/heads/main@{#1002911}

[modify] https://crrev.com/d6df80c470aea2127368ad2d4e047a4a197b5619/DEPS

Comment 72 by sheriffbot on Thu, Jul 21, 2022, 1:31 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 73 by amyressler@google.com on Tue, Jul 26, 2022, 5:38 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 74 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

Comment 75 by hyper...@gmail.com on Mon, Aug 22, 2022, 4:08 AM EDT

I got Comment 29 by tebbi@, this bug existed in some old versions of chromium/v8 since 2017.
Some apps use old version of v8 and due to dependency they can't upgrade as soon as possible.
Is there a way to backport the fix to older version of V8, in version 7.x?
I've tried the backport, but since 7.x the code structure changed a lot, I think only who familiar with V8 can achieve this.

Comment 76 by tebbi@chromium.org on Mon, Aug 22, 2022, 6:37 AM EDT Project Member

The easiest workaround is to disable escape analysis completely, by passing `--no-turbo-escape` or by changing the default flag value in `flag-definitions.h`.

Comment 77 by hyper...@gmail.com on Mon, Aug 22, 2022, 6:42 AM EDT

Thanks a lot tebbi, point a way for me. I'll give a try.