

☆ Starred by 4 users

Owner:

neis@chromium.org


CC:

gsat...@chromium.org

tebbi@chromium.org


neis@chromium.org

verwa...@chromium.org

 mstarzinger@chromium.org

achuith@chromium.org

vahl@chromium.org

 ecmziegler@google.com

Status:

Fixed (Closed)

Components:

Blink>JavaScript

Blink>JavaScript>Compiler

Modified:

Apr 21, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

2020-01-14

OS:

Linux, Android, Windows, Chrome, Mac, Fuchsia

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review

reward-2000

Security_Impact-Stable

Security_Severity-High

allpublic

reward-inprocess

Via-Wizard-Security

CVE_description-submitted

M-79

merge-merged-8.0

Release-0-M80

CVE-2020-6382

Issue 1031909: SIGTRAP hit in JIT code (Builtins_InterpreterEntryTrampoline)

Reported by taraf...@gmail.com on Sun, Dec 8, 2019, 3:17 PM EST

 Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36

Steps to reproduce the problem:
The following PoC found by fuzzing crashes v8 8.0.0 with a trap.
Run with the debug build of d8.

```
function opt() {
  var arr = [0, 0, 0];
  var j = 11;
  for (let i = 0; i < 100; i++) {
    if (i == 90) {
      i = j.toPrecision().trimLeft();
      ++arr[j];
      arr[Math.atan(i)] = 1;
    }
  }
}
```

```
function main() {
  for (let i = 0; i < 100; i++) {
    opt();
  }
}
```

main();

What is the expected behavior?

What went wrong?
Run in gdb, we can get:

Thread 1 "d8" received signal SIGTRAP, Trace/breakpoint trap.
0x00007e8a14e42dba in ?? ()

```
(gdb) x/4i $pc-0x7
0x7e8a14e42db3:   jne  0x7e8a14e42f75
0x7e8a14e42db9:   int3
=> 0x7e8a14e42dba:   xor   %r11d,%r11d
0x7e8a14e42dbd:   push  %r11
```

From our study, we think this should be different issue from 1028862.

Did this work before? N/A

Chrome version: 78.0.3904.108 Channel: stable
OS Version:
Flash Version:

Found by Soyeon Park and Wen Xu from SSLab, Gatech

[Comment 1](#) by [ClusterFuzz](#) on Mon, Dec 9, 2019, 11:24 AM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5979084169281536>.

[Comment 2](#) by [ClusterFuzz](#) on Mon, Dec 9, 2019, 11:33 AM EST

Testcase 5979084169281536 failed to reproduce the crash. Please inspect the program output at <https://clusterfuzz.com/testcase?key=5979084169281536>.

[Comment 3](#) by metzman@chromium.org on Mon, Dec 9, 2019, 3:08 PM EST

Status: Assigned (was: Unconfirmed)

Owner: mstarzinger@chromium.org

Labels: Security_Severity-High OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

Components: Blink>JavaScript

I was able to repro this locally.

Labelling this high since it seems like it could lead to renderer code execution.

Assigning to v8 sheriff. mstarzinger@ could you please take a look or find an appropriate owner?

[Comment 4](#) by metzman@chromium.org on Mon, Dec 9, 2019, 3:08 PM EST

Labels: Pri-1

[Comment 5](#) by mstarzinger@chromium.org on Tue, Dec 10, 2019, 7:04 AM EST

Owner: neis@chromium.org

Cc: mstarzinger@chromium.org tebbi@chromium.org verwa...@chromium.org gsat...@chromium.org

Components: Blink>JavaScript>Compiler

Reproduces with a regular local x64.debug build. I am not sure why CF has a hard time reproducing, I hope it isn't getting confused by the SIGTRAP again, because that would be a bummer. I ran a local bisect and ended up with the following first bad commit. Georg, since Sathya is OOO and the int3 in question happens in optimized code, could you help find the appropriate owner for this?

commit a1a45f4caa5bd47948347eaf4b736b400dfbae55

Author: Sathya Gunasekaran <gsathya@chromium.org>

Date: Wed Oct 16 14:06:24 2019 +0100

[ic] KeyedLoadIC: Optimize string keys as ArrayIndex

Updates CSA::TryToIntptr to handle array indices that are less than
INT_MAX which allows to handle string keys in the ICs.

Updates ICs to go monomorphic for string keys that are array indices.

Updates Turbofan to handle array indices when lowering element access.

Change-Id: Ibdde20130e075d0d645ab4a8266a968335eaad84

~~Bug-v8-9449~~

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+1813018>

Reviewed-by: Tobias Tebbi <tebbi@chromium.org>

Reviewed-by: Toon Verwaest <verwaest@chromium.org>

Reviewed-by: Georg Neis <neis@chromium.org>

Commit-Queue: Sathya Gunasekaran <gsathya@chromium.org>

Cr-Commit-Position: refs/heads/master@{#64320}

[Comment 6](#) by mmoroz@chromium.org on Tue, Dec 10, 2019, 11:24 AM EST

Labels: Security_Impact-Stable M-79

[Comment 7](#) by sheriffbot@chromium.org on Mon, Dec 23, 2019, 9:10 AM EST

neis: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

[Comment 8](#) Deleted

[Comment 9](#) by tebbi@chromium.org on Mon, Dec 23, 2019, 10:44 AM EST

I investigated the issue: The root cause is a wrong reduction in RedundancyElimination::ReduceSpeculativeNumberOperation where we remove a SpeculativeToNumber node while widening the type. This can lead to issues because by removing it we no longer deopt, making the type information unreliable.

It is possible that this is exploitable.

The bug has been around for more than a year already.

I'm going on holiday now so I don't have time to land a fix anymore. The fix would look like this, I don't want to upload it unnecessarily early without being able to land and backmerge in time.

```
--- a/src/compiler/redundancy-elimination.cc
+++ b/src/compiler/redundancy-elimination.cc
@@@ -385,7 +385,8 @@@ Reduction RedundancyElimination::ReduceSpeculativeNumberOperation(Node* node) {
    // than the type of the {first} node, otherwise we
    // would end up replacing NumberConstant inputs with
    // CheckBounds operations, which is kind of pointless.
-   if (!NodeProperties::GetType(first).Is(NodeProperties::GetType(check))) {
+   if (!NodeProperties::GetType(first).Is(NodeProperties::GetType(check)) &&
+       NodeProperties::GetType(check).Is(NodeProperties::GetType(first))) {
        NodeProperties::ReplaceValueInput(node, check, 0);
    }
}
```

[Comment 10](#) by sheriffbot@chromium.org on Mon, Jan 6, 2020, 9:10 AM EST

neis: Uh oh! This issue still open and hasn't been updated in the last 28 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

[Comment 11](#) by [bugdroid](#) on Tue, Jan 7, 2020, 7:39 AM EST

The following revision refers to this bug:
<https://chromium.googlesource.com/v8/v8.git/+3f7e99ac460c3ca689aac76c39bfd1852c9a7be>

commit [3f7e99ac460c3ca689aac76c39bfd1852c9a7be](#)

Author: Tobias Tebbi <tebbi@chromium.org>

Date: Tue Jan 07 12:38:05 2020

[turbofan] fix type widening bug in RedundancyElimination

[Bug-chromium:1034000](#)

Change-Id: [Ibf120d722a8cb6eb9b9eaa15163cb7846dab64ea](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+1981507>

Reviewed-by: Michael Stanton <mvstanton@chromium.org>

Commit-Queue: Tobias Tebbi <tebbi@chromium.org>

Cr-Commit-Position: refs/heads/master@{#65599}

[modify] <https://crrev.com/3f7e99ac460c3ca689aac76c39bfd1852c9a7be/src/compiler/redundancy-elimination.cc>

[Comment 12](#) by clemensb@chromium.org on Fri, Jan 10, 2020, 6:59 AM EST

Cc: neis@chromium.org

[Issue-1030444](#) has been merged into this issue.

[Comment 13](#) by adetaylor@google.com on Fri, Jan 10, 2020, 2:30 PM EST

tebbi@ if this is fixed, please mark as such. Sheriffbot will want this backported to M80 and (in due course) M79. If you think it's not exploitable or is too risky to merge, please comment thusly.

[Comment 14](#) by neis@chromium.org on Mon, Jan 13, 2020, 5:02 AM EST

Status: Fixed (was: Assigned)

Thanks Tobias!

[Comment 15](#) by tebbi@chromium.org on Mon, Jan 13, 2020, 6:56 AM EST

Labels: Merge-Request-80

It is very safe to back-merge. It might be exploitable, hard to say. In principle such typing bugs can lead to exploits and have lead to exploits historically. As neis@ just told me, my fix is incomplete though. I'll write a more complete CL and we can back-merge both.

[Comment 16](#) by sheriffbot@chromium.org on Mon, Jan 13, 2020, 6:57 AM EST

Labels: -Merge-Request-80 Merge-Review-80 Hotlist-Merge-Review

This bug requires manual review: M80's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: <https://goto.google.com/chrome-release-branch-merge-guidelines>
- Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: govind@(Android), Kariahda@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

[Comment 17](#) by [bugdroid](#) on Mon, Jan 13, 2020, 7:19 AM EST

The following revision refers to this bug:
<https://chromium.googlesource.com/v8/v8.git/+69b195c935b28857ee8e85c22af14837a0ce2c62>

commit [69b195c935b28857ee8e85c22af14837a0ce2c62](#)

Author: Tobias Tebbi <tebbi@chromium.org>

Date: Mon Jan 13 12:18:45 2020

[turbofan] fix type widening bug in RedundancyElimination, completely

This is an improved version of

<https://chromium-review.googlesource.com/c/v8/v8/+1981507>

[Bug-chromium:1034000](#)

Change-Id: [I552f49bf87340eee3c85fa02893b8e63a77a3608](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+1997129>

Reviewed-by: Georg Neis <neis@chromium.org>

Commit-Queue: Tobias Tebbi <tebbi@chromium.org>

Cr-Commit-Position: refs/heads/master@{#65722}

[modify] <https://crrev.com/69b195c935b28857ee8e85c22af14837a0ce2c62/src/compiler/redundancy-elimination.cc>

[Comment 18](#) by tebbi@chromium.org on Mon, Jan 13, 2020, 7:20 AM EST

1. Yes
2. <https://chromium-review.googlesource.com/c/v8/v8/+1981507>
<https://chromium-review.googlesource.com/c/v8/v8/+1997129>
3. the first CL yes, the second CL not yet.
4. It's a security issue that's potentially exploitable and has been in the code for a long time.
5. no

[Comment 19](#) by sheriffbot@chromium.org on Mon, Jan 13, 2020, 10:42 AM EST

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

[Comment 20](#) by srinivassista@google.com on Mon, Jan 13, 2020, 12:13 PM EST

NextAction: 2020-01-14

neis@ pls confirm here when the second CL is also ready to back port. I will approve both the CL's at the same time

[Comment 21](#) by neis@chromium.org on Tue, Jan 14, 2020, 9:02 AM EST
It's ready (looking good in 81.0.4027.0).

[Comment 22](#) by srinivassista@google.com on Tue, Jan 14, 2020, 11:54 AM EST
Labels: -Merge-Review-80 Merge-Approved-80
merge approved fro M80, branch:3987 pls complete your merge to branch asap.

[Comment 23](#) by natashapabrai@google.com on Tue, Jan 14, 2020, 11:56 AM EST
Labels: reward-topanel

[Comment 24](#) by gov...@chromium.org on Tue, Jan 14, 2020, 12:16 PM EST
Please merge your change to M80 branch 3987 ASAP so we can pick it up for tomorrow's beta release, we're cutting Beta RC soon. Thank you.

[Comment 25](#) by [bugdroid](#) on Wed, Jan 15, 2020, 5:44 AM EST
Labels: merge-merged-8.0
The following revision refers to this bug:
<https://chromium.googlesource.com/v8/v8.git/+9276af78f87a4e7160d67afca01239070f47e5a6>

commit [9276af78f87a4e7160d67afca01239070f47e5a6](#)
Author: Georg Neis <neis@chromium.org>
Date: Wed Jan 15 10:43:58 2020

Merged: Squashed multiple commits.

Merged: [turbofan] fix type widening bug in RedundancyElimination
Revision: [3f7e99ac460c3ca689aac76c39fbd1852c9a7be](#)

Merged: [turbofan] fix type widening bug in RedundancyElimination, completely
Revision: [69b195c935b28857ee8e85c22af14837a0ce2c62](#)

[BUG=chromium:4034000](#)
NOTRY=true
NOPRESUBMIT=true
NOTRECHECKS=true
R=tebbi@chromium.org

Change-Id: I938a5ad9c1b9f7bd345311f44d815f5e49dc08df
Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8+/2002388>
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Georg Neis <neis@chromium.org>
Cr-Commit-Position: refs/branch-heads/8.0@(#22)
Cr-Branched-From: [69827db645f6ce065bf16a795a4ec8d3a51057f](#)-refs/heads/8.0.426@(#2)
Cr-Branched-From: [2fe1552c5809d0dd92e81d36a5535cbb7c518800](#)-refs/heads/master@(#65318)

[modify] <https://crrev.com/9276af78f87a4e7160d67afca01239070f47e5a6/src/compiler/redundancy-elimination.cc>

[Comment 26](#) by neis@chromium.org on Wed, Jan 15, 2020, 5:55 AM EST
Labels: -Merge-Approved-80

[Comment 27](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 4:21 PM EST
Labels: -reward-topanel reward-unpaid reward-2000

*** 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 28](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 4:31 PM EST
Congrats the Panel decided to reward \$2,000 for this report!

[Comment 29](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 5:04 PM EST
Labels: -reward-unpaid reward-inprocess

[Comment 30](#) by adetaylor@google.com on Sat, Feb 1, 2020, 8:13 PM EST
Labels: Release-0-M80

[Comment 31](#) by adetaylor@chromium.org on Mon, Feb 3, 2020, 6:46 PM EST
Labels: CVE-2020-6382 CVE_description-missing

[Comment 32](#) by adetaylor@chromium.org on Mon, Feb 10, 2020, 4:35 PM EST
Labels: -CVE_description-missing CVE_description-submitted

[Comment 33](#) by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST
Cc: achuith@chromium.org

[Comment 34](#) by [sheriffbot](#) on Tue, Apr 21, 2020, 2:55 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