Starred by 1 user

Owner:	neis@chromium.org
CC:	tebbi@chromium.org vahl@chromium.org ecmziegler@google.com
Status:	Verified *(Closed)*
Components:	Blink>JavaScript>Compiler
Modified:	Dec 21, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
Target-85
M-85
FoundIn-85
FoundIn-86
Release-0-M86
merge-merged-8.6
CVE-2020-15979

Issue 1127319: Security: Debug check failed: IrOpcode::IsInlineeOpcode(node->opcode()).

Reported by b3nd3...@gmail.com on Fri, Sep 11, 2020, 8:17 AM EDT

Code

Target : ASAN-D8-DBG Latest
Crash Type: Fatal error in ../../src/compiler/js-inlining.cc, line 378
Crash State:

```
#
# Fatal error in ../../src/compiler/js-inlining.cc, line 378
# Debug check failed: IrOpcode::IsInlineeOpcode(node->opcode()).
#
#
```

POC:

```
----------------------------
function main() {
function v1(v2,v3) {
    const v4 = Reflect;
    const v8 = [11.11,11.11,11.11];
    const v10 = {__proto__:1111,a:-1,c:RegExp,constructor:v8,d:1111,toString:-1};
    const v12 = [11.11,11.11,11.11];
    function v13(v14,v15) {}
    const v16 = {apply:v13,call:v13,construct:v13,deleteProperty:v13,getOwnPropertyDescriptor:v13,getPrototypeOf:v13,has:v13,isExtensible:v13,set:v13,setPrototypeOf:v13};
}
function v19(v20,v21) {
    let v22 = Number;
    v22 = v1;
    const v23 = +0;
    if (v23) {
        void(v22 = Number);
    } else {
        function v24(v25,v26) {
            const v28 = ".Cactus"[0];
            for (let v32 = 0; v32 < 7; v32++) {}
        }
        void(new Promise(v24));
        const v36 = [1337,1337,1337];
        try {
            for (const v37 of v36) {
                const v38 = cactus;
                const v56 = [v50,13.37];
                const v58 = [cactus,cactus,[] = cactus] = v117;
            }
        } catch(v119) {
        }
    }
```

```
    const v120 = v22(0);
}
for (let v124 = 0; v124 < 100; v124++) {
    const v125 = v19();
}
}
main();
----------------------------


*** - runtime flags - (--interrupt-budget=1024)
----
*** This sample was found through context aware fuzzing .
*** Fuzzer Generation - MK_0.312 .
```

Comment 1 Deleted

Comment 2 by ClusterFuzz on Fri, Sep 11, 2020, 5:12 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5703016175173632.

Comment 3 by ClusterFuzz on Fri, Sep 11, 2020, 5:21 PM EDT

Labels: OS-Linux

Comment 4 by ClusterFuzz on Fri, Sep 11, 2020, 5:29 PM EDT

Labels: OS-Mac

Comment 5 by jdeblasio@chromium.org on Fri, Sep 11, 2020, 5:29 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: neis@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Android OS-Chrome OS-Fuchsia OS-Windows
Components: Blink>JavaScript>Compiler

neis@: can you PTAL and route appropriately? Thanks!

Comment 6 by ClusterFuzz on Fri, Sep 11, 2020, 5:37 PM EDT

Labels: FoundIn-86 FoundIn-85

Detailed Report: https://clusterfuzz.com/testcase?key=5703016175173632

Fuzzer: None
Job Type: linux_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
  IrOpcode::IsInlineeOpcode(node->opcode()) in js-inlining.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=62274:62275

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5703016175173632

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5703016175173632 -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 7 by sheriffbot on Sat, Sep 12, 2020, 1:57 PM EDT

Labels: Target-85 M-85

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 8 by sheriffbot on Sat, Sep 12, 2020, 2:38 PM EDT

Labels: 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 9 by neis@chromium.org on Mon, Sep 14, 2020, 2:47 AM EDT

Status: Started (was: Assigned)

Thanks for reporting! So far it looks non-exploitable as a CHECK failure will happen shortly after in a release build.

Comment 10 by neis@chromium.org on Mon, Sep 14, 2020, 4:51 AM EDT

Cc: tebbi@chromium.org

Comment 11 by bugdroid on Mon, Sep 14, 2020, 8:03 AM EDT

The following revision refers to this bug:
  https://chromium.googlesource.com/v8/v8.git/+/219b28bfe2ea76de63f034eb75b67e8ded339d94

commit 219b28bfe2ea76de63f034eb75b67e8ded339d94
Author: Georg Neis <neis@chromium.org>
Date: Mon Sep 14 12:01:55 2020

[turbofan] Fix bug in inlining

JSInliningHeuristic::Finalize did not take into account that by the
time it gets called some of the candidate nodes may have changed to
non-call operators.

~~Bug: chromium:1127319~~
Change-Id: I180ed36de98455be6b55790ba7bdb4391ff5fd5c
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2409273
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Georg Neis <neis@chromium.org>
Auto-Submit: Georg Neis <neis@chromium.org>
Cr-Commit-Position: refs/heads/master@{#69874}

[modify] https://crrev.com/219b28bfe2ea76de63f034eb75b67e8ded339d94/src/compiler/js-inlining-heuristic.cc
[add] https://crrev.com/219b28bfe2ea76de63f034eb75b67e8ded339d94/test/mjsunit/compiler/regress-1127319.js

Comment 12 by neis@chromium.org on Mon, Sep 14, 2020, 8:32 AM EDT

Status: Fixed (was: Started)
Labels: -Security_Severity-High Security_Severity-Medium

I'm keeping it as a security bug since I don't see a guarantee that the CHECK mentioned earlier fails.

Comment 13 by ClusterFuzz on Mon, Sep 14, 2020, 8:34 AM EDT

Detailed Report: https://clusterfuzz.com/testcase?key=5703016175173632

Fuzzer: None
Job Type: linux_d8_dbg
Platform Id: linux

Crash Type: DCHECK failure
Crash Address:
Crash State:
  IrOpcode::IsInlineeOpcode(node->opcode()) in js-inlining.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=62274:62275

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5703016175173632

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5703016175173632 -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 14 by ClusterFuzz on Mon, Sep 14, 2020, 8:47 AM EDT

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

ClusterFuzz testcase 5703016175173632 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_d8_dbg&range=69873:69874

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

Comment 15 by adetaylor@google.com on Mon, Sep 14, 2020, 2:31 PM EDT

Labels: reward-topanel

Comment 16 by adetaylor@chromium.org on Mon, Sep 14, 2020, 2:34 PM EDT

neis@ for the sake of the VRP panel, please could you describe what would have happened here on a release build if it had gone past the DCHECK?

Comment 17 by sheriffbot on Mon, Sep 14, 2020, 3:08 PM EDT

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

Comment 18 by sheriffbot on Tue, Sep 15, 2020, 3:35 PM EDT

Labels: Merge-Request-86

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M86. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

Comment 19 by sheriffbot on Tue, Sep 15, 2020, 3:40 PM EDT

Labels: -Merge-Request-86 Hotlist-Merge-Review Merge-Review-86

This bug requires manual review: M86'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://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- 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), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 20 by neis@chromium.org on Wed, Sep 16, 2020, 3:14 AM EDT

Re #16:
In the submitted code snippet, a release build will abort a little later with a failing CHECK. As I mentioned in one of my comments, however, I don't think that CHECK is guaranteed to fail in general. I could imagine optimization failing due to other CHECKs or due to segfaulting on OOB reads in C++ code. I could also imagine optimization succeeding and producing an incorrect but non-malicious program. I don't see how a malicious program could be generated but I don't dare to rule it out.

Comment 21 by adetaylor@google.com on Wed, Sep 16, 2020, 7:15 PM EDT

Labels: -reward-topanel reward-unpaid reward-5000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 22 by adetaylor@google.com on Wed, Sep 16, 2020, 7:21 PM EDT

Congratulations! Our VRP panel decided to award $5,000 for this report.

Comment 23 by neis@chromium.org on Thu, Sep 17, 2020, 7:31 AM EDT

Re #19:
1) yes
2) the commit in #11
3) it's in canary 4265 but v8 in that canary is broken for other reasons, 4267 should be good to check
4) bug fix, potentially security relevant
5) no

Comment 24 by adetaylor@google.com on Thu, Sep 17, 2020, 4:29 PM EDT

Labels: -Merge-Review-86 Merge-Approved-86

Approving merge to M86, branch 4240.

Comment 25 by gov...@chromium.org on Thu, Sep 17, 2020, 6:12 PM EDT

Please merge your change to M86 branch 4240 ASAP. Thank you.

Comment 26 by bugdroid on Fri, Sep 18, 2020, 3:06 AM EDT

Labels: merge-merged-8.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8.git/+/abb4d0a431c0d3fb1f67eaf04c3a8bf1925f9b28

commit abb4d0a431c0d3fb1f67eaf04c3a8bf1925f9b28
Author: Georg Neis <neis@chromium.org>
Date: Fri Sep 18 07:05:30 2020

Merged: [turbofan] Fix bug in inlining

Revision: 219b28bfe2ea76de63f034eb75b67e8ded339d94

~~BUG=chromium:1127319~~
NOTRY=true
NOPRESUBMIT=true
NOTREECHECKS=true
R=tebbi@chromium.org

Change-Id: I98e77bac81e2cf822a4a4987115e0cf01b1dbc52
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/2416383
Reviewed-by: Tobias Tebbi <tebbi@chromium.org>
Commit-Queue: Georg Neis <neis@chromium.org>
Cr-Commit-Position: refs/branch-heads/8.6@{#12}
Cr-Branched-From: a64aed2333abf49e494d2a5ce24bbd14fff19f60-refs/heads/8.6.395@{#1}
Cr-Branched-From: a626bc036236c9bf92ac7b87dc40c9e538b087e3-refs/heads/master@{#69472}

[modify] https://crrev.com/abb4d0a431c0d3fb1f67eaf04c3a8bf1925f9b28/src/compiler/js-inlining-heuristic.cc
[add] https://crrev.com/abb4d0a431c0d3fb1f67eaf04c3a8bf1925f9b28/test/mjsunit/compiler/regress-1127319.js

Comment 27 by neis@chromium.org on Fri, Sep 18, 2020, 3:07 AM EDT

Labels: -Merge-Approved-86

Comment 28 by adetaylor@google.com on Thu, Sep 24, 2020, 1:35 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 29 by adetaylor@google.com on Thu, Oct 1, 2020, 3:47 PM EDT

Labels: Release-0-M86

Comment 30 by adetaylor@google.com on Mon, Oct 5, 2020, 1:00 AM EDT

Labels: CVE-2020-15979 CVE_description-missing

Comment 31 by adetaylor@google.com on Mon, Nov 2, 2020, 9:15 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Mon, Dec 21, 2020, 1:50 PM EST

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