


☆ Starred by 2 users

Owner: ishell@chromium.org

CC: leszek@chromium.org
vahl@chromium.org
 ecmziegler@google.com

Status: Fixed (Closed)

Components: [Blink>JavaScript](#)

Modified: Jul 15, 2021

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: [Linux, Windows](#)

Pri: [2](#)

Type: [Bug-Security](#)

[Security_Severity-Low](#)
[Security_Impact-Stable](#)
[allpublic](#)
[reward-inprocess](#)
[reward-15000](#)
[CVE_description-submitted](#)
[M-89](#)
[M-87](#)
[M-90](#)
[M-88](#)
[external_security_report](#)
[Release-0-M91](#)
[CVE-2021-30536](#)

Issue 1194358: Security: OOB in v8

Reported by chris...@gmail.com on Wed, Mar 31, 2021, 1:31 AM EDT

 Code

The attached poc triggers an OOB access in 32bit x86 builds of v8. Run with --stress-compaction
Note that the crash can still be hit with a more complicated poc without that flag.

The problem in src/builtins/ia32/builtins-ia32.cc in the function Generate_PushBoundArguments
The stack overflow check fails to set up a proper frame

```
...  
    FrameScope frame(masm, StackFrame::MANUAL);  
    __ CallRuntime(Runtime::kThrowStackOverflow);  
...
```

The fix is to add the following line between the two.
__ EnterFrame(StackFrame::INTERNAL);

As such the return address will be interpreted as an object during stack walking by the GC.
The crashing address can be controlled by having the return address point to jitted code. The code will then be interpreted as an address.

In the attached poc it will crash at addresses like these
Received signal 11 SEGV_MAPERR 000041406815

CREDIT INFORMATION

Reporter credit: Chris Salls (@salls)

poc.js
465 bytes [View](#) [Download](#)

[Comment 1](#) by [sheriffbot](#) on Wed, Mar 31, 2021, 1:32 AM EDT [Project Member](#)

Labels: [external_security_report](#)

[Comment 2](#) by [ClusterFuzz](#) on Wed, Mar 31, 2021, 8:14 PM EDT [Project Member](#)

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5680271408824320>.

[Comment 3](#) by dubery@chromium.org on Wed, Mar 31, 2021, 8:40 PM EDT [Project Member](#)

Status: Assigned (was: Unconfirmed)

Owner: ishell@chromium.org

ClusterFuzz failed to reproduce the bug, but I suspect that's due to the 32-bit requirement, as this looks plausible. ishell@ - can you help triage?

[Comment 4](#) by ishell@chromium.org on Thu, Apr 1, 2021, 10:14 AM EDT [Project Member](#)

Status: Started (was: Assigned)
Cc: leszeks@chromium.org
Labels: OS-Linux OS-Windows
Components: Blink>JavaScript

Thank you for the report and suggestion for the fix!

Not sure how exploitable this crash is but it does happen without any flags.

[Comment 5](#) by [Git Watcher](#) on Thu, Apr 1, 2021, 11:40 AM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/v8/v8+/8809cb11e206bd7b0bea5f36f9a5c7cc401cb65a>

commit [8809cb11e206bd7b0bea5f36f9a5c7cc401cb65a](#)

Author: Igor Sheludko <ishell@chromium.org>

Date: Thu Apr 01 14:11:28 2021

[builtins][ia32] Create internal frame before throwing StackOverflow

... in CallBoundFunction builtin.

[Bug: chromium:1404268](#)

Change-Id: I8ddd4ff39cf399d4af332cff8eddc40e217cfdb

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8+/2800111>

Auto-Submit: Igor Sheludko <ishell@chromium.org>

Reviewed-by: Leszek Swirski <leszeks@chromium.org>

Commit-Queue: Igor Sheludko <ishell@chromium.org>

Cr-Commit-Position: refs/heads/master@{#73775}

[modify] <https://crrev.com/8809cb11e206bd7b0bea5f36f9a5c7cc401cb65a/src/builtins/ia32/builtins-ia32.cc>

[Comment 6](#) by ishell@chromium.org on Thu, Apr 1, 2021, 11:40 AM EDT Project Member

Status: Fixed (was: Started)

[Comment 7](#) by [sheriffbot](#) on Thu, Apr 1, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

[Comment 8](#) by [sheriffbot](#) on Thu, Apr 1, 2021, 1:56 PM EDT Project Member

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

[Comment 9](#) by adetaylor@google.com on Wed, Apr 7, 2021, 3:48 PM EDT Project Member

Status: Assigned (was: Fixed)

ishell@ please can you let us know the appropriate Security_Severity and Security_Impact then mark this as Fixed again. We need those labels so it can be merged to the appropriate branches.

[Comment 10](#) by ishell@chromium.org on Wed, Apr 7, 2021, 5:57 PM EDT Project Member

Status: Fixed (was: Assigned)

Labels: Security_Impact-Stable Security_Severity-Low M-87 M-88 M-89 M-90

[Comment 11](#) by amyressler@google.com on Wed, Apr 7, 2021, 6:52 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-15000

*** 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 12](#) by amyressler@chromium.org on Wed, Apr 7, 2021, 7:11 PM EDT Project Member

Congratulations, Chris! The VRP Panel has decided to award you \$15,000 for this report. Thank you for your efforts and reporting this issue to us!

[Comment 13](#) by chris...@gmail.com on Thu, Apr 8, 2021, 5:26 AM EDT

Thanks for the award!

[Comment 14](#) by [sheriffbot](#) on Thu, Apr 8, 2021, 1:44 PM EDT Project Member

Labels: -Pri-3 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 15](#) by amyressler@google.com on Fri, Apr 9, 2021, 11:16 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 16](#) by amyressler@chromium.org on Mon, May 24, 2021, 11:18 AM EDT Project Member

Labels: Release-0-M91

[Comment 17](#) by amyressler@google.com on Mon, May 24, 2021, 2:19 PM EDT Project Member

Labels: CVE-2021-30536 CVE_description-missing

[Comment 18](#) by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 19](#) by [sheriffbot](#) on Thu, Jul 15, 2021, 9:09 AM 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

