




☆ Starred by 2 users

**Owner:** [nicohartmann@chromium.org](mailto:nicohartmann@chromium.org)

**CC:** [adetaylor@chromium.org](mailto:adetaylor@chromium.org)  
 [benmason@chromium.org](mailto:benmason@chromium.org)  
 [hablich@chromium.org](mailto:hablich@chromium.org)  
[pbomm...@chromium.org](mailto:pbomm...@chromium.org)  
[achuith@chromium.org](mailto:achuith@chromium.org)  
[vahl@chromium.org](mailto:vahl@chromium.org)  
 [ecmziegler@google.com](mailto:ecmziegler@google.com)

**Status:** Verified (Closed)

**Components:** [Blink>JavaScript](#)  
[Blink>JavaScript>Compiler](#)

**Modified:** Mar 11, 2020

**Backlog-Rank:** ----

**Editors:** ----

**EstimatedDays:** ----

**NextAction:** ----

**OS:** [Linux, Android, Windows, Chrome, Mac, Fuchsia](#)

**Pri:** 2

**Type:** [Bug-Security](#)

[Hotlist-Merge-Review](#)  
[reward-0](#)  
[Security\\_Severity-Low](#)  
[Security\\_Impact-Stable](#)  
[M-80](#)  
[allpublic](#)  
[ClusterFuzz-Verified](#)  
[Test-Predator-Auto-Components](#)  
[CVE\\_description-submitted](#)  
[Release-0-M80](#)  
[CVE-2020-6415](#)

**Issue 1029576: Security: Debug check failed: 0 <= index && index < node->op()->ValueInputCount().**

Reported by [b3nd3...@gmail.com](mailto:b3nd3...@gmail.com) on Sat, Nov 30, 2019, 5:59 AM EST

 Code

Target : ASAN-D8-DBG Latest  
Crash Type:Debug check failed  
Crash State:

```
#
# Fatal error in ../../src/compiler/node-properties.cc, line 57
# Debug check failed: 0 <= index && index < node->op()->ValueInputCount().
#
#
#
#FailureMessage Object: 0x7ffa8a2e750
```

POC:

```
-----
function main() {
  function v0(v1,v2) {
    let v5 = 0;
    do {
      const v9 = [1000.0];
      const v11 = {};
      const v12 = [v9,v11,v11,v11,v11];
      const v13 =
{deleteProperty:v9.has:1000.0,setPrototypeOf:Intl.apply:v9.isExtensible:v11.set:v11.preventExtensions:v12.get:v12.getOwnPropertyDescriptor:v12.getPrototypeOf:v9.defineP
roperty:10000.ownKeys:1337.construct:10000};
      const v15 = new Proxy(Intl,v13);
      try {
        const v18 =
{setPrototypeOf:BigInt.ownKeys:BigInt.has:BigInt.preventExtensions:Object.getPrototypeOf:BigInt.call:v15.isExtensible:v15.apply:Object.get:v15.getOwnPropertyDescriptor:
Object};
        const v20 = new Proxy(v11,v18);
        const v21 = BigInt.asUintN(v20);
      } catch(v22) {
      }
    } while (v5 < 8);
  }
  const v23 = v0();
}
main();
-----
```

\*\*\* This sample was found through context aware fuzzing .

Comment 1 by ClusterFuzz on Mon, Dec 2, 2019, 5:09 PM EST Project Member  
ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=4699684731748352>.

Comment 2 by palmer@chromium.org on Mon, Dec 2, 2019, 5:11 PM EST Project Member  
Owner: bmeu...@chromium.org  
Labels: M-80 OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1  
Components: Blink>JavaScript  
bmeurer: Is this is a DCHECK that should be a run-time, production check?

Comment 3 by palmer@chromium.org on Mon, Dec 2, 2019, 5:12 PM EST Project Member  
Labels: Security\_Impact-Stable

Comment 4 by palmer@chromium.org on Mon, Dec 2, 2019, 5:14 PM EST Project Member  
Status: Assigned (was: Unconfirmed)

Comment 5 by ClusterFuzz on Mon, Dec 2, 2019, 6:34 PM EST Project Member  
Labels: Test-Predator-Auto-Components  
Components: Blink>JavaScript>Compiler  
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 Mon, Dec 2, 2019, 6:34 PM EST Project Member  
Detailed Report: <https://clusterfuzz.com/testcase?key=4699684731748352>

Fuzzer:  
Job Type: linux\_asan\_d8\_dbg  
Platform Id: linux  
  
Crash Type: DCHECK failure  
Crash Address:  
Crash State:  
0 <= index && index < node->op()->ValueInputCount() in node-properties.cc  
v8::internal::compiler::NodeProperties::GetValueInput  
v8::internal::compiler::JSCallReducer::ReduceBigIntAsUIntN  
  
Sanitizer: address (ASAN)  
  
Regressed: [https://clusterfuzz.com/revisions?job=linux\\_asan\\_d8\\_dbg&range=62487:62488](https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=62487:62488)  
  
Reproducer Testcase: [https://clusterfuzz.com/download?testcase\\_id=4699684731748352](https://clusterfuzz.com/download?testcase_id=4699684731748352)  
  
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/4699684731748352> -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 neis@chromium.org on Tue, Dec 3, 2019, 5:05 AM EST Project Member  
Owner: nicohartmann@chromium.org  
Cc: bmeu...@chromium.org

Comment 8 by bugdroid on Tue, Dec 3, 2019, 10:59 AM EST Project Member  
The following revision refers to this bug:  
<https://chromium.googlesource.com/v8/v8.git/+e76d29b35e8341795c4e8f8463a90d33fb1cb68a>

commit e76d29b35e8341795c4e8f8463a90d33fb1cb68a  
Author: Nico Hartmann <[nicohartmann@chromium.org](mailto:nicohartmann@chromium.org)>  
Date: Tue Dec 03 15:58:07 2019

[Turbofan] Fixes crash on missing BigInt.asUIntN argument

~~Bug=chromium-1029576~~  
Change-Id: If647f764da2682a0f278b9b8060d0665fab1c40c  
Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8+/1948711>  
Commit-Queue: Georg Neis <[neis@chromium.org](mailto:neis@chromium.org)>  
Auto-Submit: Nico Hartmann <[nicohartmann@chromium.org](mailto:nicohartmann@chromium.org)>  
Reviewed-by: Georg Neis <[neis@chromium.org](mailto:neis@chromium.org)>  
Cr-Commit-Position: refs/heads/master@{#65312}

[modify] <https://crrev.com/e76d29b35e8341795c4e8f8463a90d33fb1cb68a/src/compiler/js-call-reducer.cc>  
[add] <https://crrev.com/e76d29b35e8341795c4e8f8463a90d33fb1cb68a/test/mjsunit/regress/regress-1029576.js>

Comment 9 by ClusterFuzz on Wed, Dec 4, 2019, 3:38 AM EST Project Member  
Detailed Report: <https://clusterfuzz.com/testcase?key=4699684731748352>

Fuzzer:  
Job Type: linux\_asan\_d8\_dbg  
Platform Id: linux  
  
Crash Type: DCHECK failure  
Crash Address:  
Crash State:  
0 <= index && index < node->op()->ValueInputCount() in node-properties.cc  
v8::internal::compiler::NodeProperties::GetValueInput  
v8::internal::compiler::JSCallReducer::ReduceBigIntAsUIntN  
  
Sanitizer: address (ASAN)

Regressed: [https://clusterfuzz.com/revisions?job=linux\\_asan\\_d8\\_dbg&range=62487:62488](https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=62487:62488)

Reproducer Testcase: [https://clusterfuzz.com/download?testcase\\_id=4699684731748352](https://clusterfuzz.com/download?testcase_id=4699684731748352)

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/4699684731748352> -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 10** by [ClusterFuzz](#) on Wed, Dec 4, 2019, 4:02 AM EST Project Member

**Status:** Verified (was: Assigned)

**Labels:** ClusterFuzz-Verified

ClusterFuzz testcase 4699684731748352 is verified as fixed in [https://clusterfuzz.com/revisions?job=linux\\_asan\\_d8\\_dbg&range=65311:65312](https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=65311:65312)

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

**Comment 11** by [nicohartmann@chromium.org](mailto:nicohartmann@chromium.org) on Wed, Dec 4, 2019, 4:16 AM EST Project Member

**Labels:** Merge-Request-79 Security\_Severity-High

Fixed and verified in canary. Requesting to merge back to 79.

**Comment 12** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Dec 4, 2019, 4:17 AM EST Project Member

**Labels:** -Merge-Request-79 Hotlist-Merge-Review Merge-Review-79

This bug requires manual review: We are only 5 days from stable.

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: benmason@ (Android), kariahda@ (iOS), cindyb@ (ChromeOS), govind@ (Desktop)

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

**Comment 13** by [nicohartmann@chromium.org](mailto:nicohartmann@chromium.org) on Wed, Dec 4, 2019, 5:06 AM EST Project Member

This is the Bugfix CL that needs to be merged: <https://chromium-review.googlesource.com/c/v8/v8/+1948711/1>

**Comment 14** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Dec 4, 2019, 10:42 AM EST Project Member

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

**Comment 15** by [gov...@chromium.org](mailto:gov...@chromium.org) on Wed, Dec 4, 2019, 1:18 PM EST Project Member

**Cc:** adetaylor@chromium.org pbomm...@chromium.org benmason@chromium.org

+adetaylor@ (Security TPM) , CL listed at #8 is not made it to canary (80.0.3985.0) yet and we already cut M79 Stable RC for Desktop. Can this wait for next M79 respin so by then change will be well baked in canary?

**Comment 16** by [bmeu...@chromium.org](mailto:bmeu...@chromium.org) on Wed, Dec 4, 2019, 1:20 PM EST Project Member

**Cc:** -bmeu...@chromium.org

**Comment 17** by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Dec 4, 2019, 1:38 PM EST Project Member

Sounds like it needs to wait for the first M79 stable refresh, "but" it would be good to hear comment from nicohartmann@ as well, as it's hard for me to assess the consequences if a release build sails past a V8 DCHECK. What would have happened in this case? Type confusion? Does it appear as though it would have been readily exploitable?

**Comment 18** by [gov...@chromium.org](mailto:gov...@chromium.org) on Wed, Dec 4, 2019, 1:40 PM EST Project Member

**Cc:** hablich@chromium.org

+hablich@ (V8 TPM) as well.

**Comment 19** by [nicohartmann@chromium.org](mailto:nicohartmann@chromium.org) on Thu, Dec 5, 2019, 5:09 AM EST Project Member

Investigated the consequences in release builds. It turns out the generated code just deopts, so it is not a security vulnerability.

**Comment 20** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Thu, Dec 5, 2019, 12:23 PM EST Project Member

**Labels:** -Security\_Severity-High -Merge-Review-79 Security\_Severity-Low

Great! In that case I'm going to set this to severity low (just in case it has any residual unexpected impact, I'd like to keep it as a security bug). So no need to merge.

**Comment 21** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Fri, Dec 6, 2019, 10:30 AM EST 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 22** by [awhalley@chromium.org](mailto:awhalley@chromium.org) on Wed, Dec 11, 2019, 5:53 PM EST Project Member

**Labels:** reward-topanel

**Comment 23** by [adetaylor@google.com](mailto:adetaylor@google.com) on Tue, Jan 28, 2020, 3:12 PM EST Project Member

[b3nd3rm3@gmail.com](mailto:b3nd3rm3@gmail.com) - how would you like to be credited in the release notes?

NB for VRP panel per #c19 this is believed not exploitable, but I wanted to treat it as a security bug in case there were unforeseen implications.

**Comment 24** by [b3nd3...@gmail.com](mailto:b3nd3...@gmail.com) on Wed, Jan 29, 2020, 1:33 AM EST

#23 Credits are for - Avihay Cohen @ SeraphicAlgorithms . Thanks

Comment 25 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, Jan 29, 2020, 11:57 AM EST Project Member  
Thanks.

Comment 26 by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Jan 29, 2020, 7:06 PM EST Project Member  
**Labels:** -reward-to-panel reward-0  
Unfortunately the Panel declined to reward this report

Comment 27 by [adetaylor@google.com](mailto:adetaylor@google.com) on Sat, Feb 1, 2020, 8:13 PM EST Project Member  
**Labels:** Release-0-M80

Comment 28 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 3, 2020, 6:49 PM EST Project Member  
**Labels:** CVE-2020-6415 CVE\_description-missing

Comment 29 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 10, 2020, 4:37 PM EST Project Member  
**Labels:** -CVE\_description-missing CVE\_description-submitted

Comment 30 by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Mar 4, 2020, 1:44 PM EST Project Member  
**Cc:** [achuith@chromium.org](mailto:achuith@chromium.org)

Comment 31 by [sheriffbot](#) on Wed, Mar 11, 2020, 1:58 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