

☆ Starred by 2 users

Owner:

ftang@chromium.org

CC:

adetaylor@chromium.org


jkummerow@chromium.org

janag...@google.com

js...@chromium.org

syg@chromium.org

vahl@chromium.org

 ecmziegler@google.com

Status:

Fixed (Closed)

Components:

Blink>JavaScript

Modified:

Sep 21, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Windows, Mac

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review

Reward-1000

Security_Impact-Stable

Security_Severity-Medium

allpublic

reward-inprocess

ClusterFuzz-Verified

Test-Predator-Auto-Components

Test-Predator-Auto-Owner

CVE_description-submitted

Target-90

FoundIn-89

FoundIn-90

merge-merged-4240

merge-merged-m86

M-91

LTR-Merged-86

LTS-Security-86

Target-91

external_security_report


merge-merged-4430

merge-merged-90

merge-merged-4472

Issue 1194899: BigInt toLocaleString free invalid pointer

Reported by wxmp...@gmail.com on Thu, Apr 1, 2021, 4:03 AM EDT

 Code

VULNERABILITY DETAILS

The following testcase crashes the latest debug build of d8.

VERSION

V8: V8 version 9.1.0 (candidate)
Operating System: Linux 64bit

REPRODUCTION CASE

v1 = 'MZ-65537RQZ-65537RvZ-65537RTZ-65537RdZ-65537RMZ-65537RJZ-65537ReZ-65537RpZ-65537R-Z-65537R2Z-65537R5Z-65537R6Z-65537R-2Z-65537RnZ-65537RuZ-65537RmZ';
v2 = BigInt(1);
v2.toLocaleString(v1);

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Crash State:

free(): invalid pointer
Received signal 6

#0 __GI_raise (sig=sig@entry=6) at ./sysdeps/unix/sysv/linux/raise.c:51
#1 0x00007f9abbc31921 in __GI_abort () at abort.c:79
#2 0x00007f9abbc7a967 in __libc_message (action=action@entry=do_abort, fmt=fmt@entry=0x7f9abba7b0d "%s\n") at ./sysdeps/posix/libc_fatal.c:181
#3 0x00007f9abbc819da in malloc_printerr (str=str@entry=0x7f9abba5d08 "free(): invalid pointer") at malloc.c:5342
#4 0x00007f9abbc88f0c in __int_free (have_lock=0, p=0x7ffe8b59e198, av=0x7f9abbfdcc40 <main_arena>) at malloc.c:4167
#5 __GI___libc_free (mem=0x7ffe8b59e1a8) at malloc.c:3134
#6 0x00007f9abc82fd2d in uprv_free_68 (buffer=0x7ffe8b59e1a8) at ./third_party/icu/source/common/cmemory.cpp:99
#7 0x00007f9abc85058b in icu_68::Locale::init (this=0x7ffe8b59e628, localeID=0x5618e37c5550
"mz_65537R-65537RDZ_65537REZ_65537RJZ_65537RMZ_65537RPZ_65537RQZ_65537RTZ_65537RUZ_65537RVZ@z=65537r2z-65537fz-65537r6z-65537r-2z-65537mz-65537ruz-65537rmz", canonicalize=1 '001') at ./third_party/icu/source/common/locid.cpp:1841
#8 0x00007f9abc8523d1 in icu_68::Locale::canonicalize (this=0x7ffe8b59e628, status=@0x7ffe8b59e464: U_ZERO_ERROR) at
./third_party/icu/source/common/locid.cpp:2132
#9 0x00007f9abf4698fe in v8::internal::(anonymous namespace)::CanonicalizeLanguageTag (isolate=0x5618e370af30, locale_in=...) at ./src/objects/intl-objects.cc:794
#10 0x00007f9abf462a7c in v8::internal::(anonymous namespace)::CanonicalizeLanguageTag (isolate=0x5618e370af30, locale_in=...) at ./src/objects/intl-objects.cc:844
#11 0x00007f9abf462000 in v8::internal::Intl::CanonicalizeLocaleList (isolate=0x5618e370af30, locales=..., only_return_one_result=false) at ./src/objects/intl-objects.cc:872
#12 0x00007f9abf4c9321 in v8::internal::JSNumberFormat::New (isolate=0x5618e370af30, map=..., locales=..., options_obj=..., service=0x7f9abdaeb9b0
"BigInt.prototype.toLocaleString") at ./src/objects/js-number-format.cc:827
#13 0x00007f9abf4642bb in v8::internal::(anonymous namespace)::New<v8::internal::JSNumberFormat> (isolate=0x5618e370af30, constructor=..., locales=..., options=...,
method=0x7f9abdaeb9b0 "BigInt.prototype.toLocaleString") at ./src/objects/intl-objects.cc:188
#14 0x00007f9abf463f33 in v8::internal::Intl::NumberToLocaleString (isolate=0x5618e370af30, num=..., locales=..., options=..., method=0x7f9abdaeb9b0
"BigInt.prototype.toLocaleString") at ./src/objects/intl-objects.cc:1105
#15 0x00007f9abecaa74e in v8::internal::Builtin_Impl_BigIntPrototypeToLocaleString (args=..., isolate=0x5618e370af30) at ./src/builtins/builtins-bbigint.cc:135
#16 0x00007f9abecaa31b in v8::internal::Builtin_BigIntPrototypeToLocaleString (args_length=6, args_object=0x7ffe8b5a16a0, isolate=0x5618e370af30) at
./src/builtins/builtins-bbigint.cc:126

```
#17 0x00007f9abe6a3120 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit () from /data/v8/out/Debug/libv8.so
#18 0x00007f9abe3fd16b in Builtins_InterpreterEntryTrampoline () from /data/v8/out/Debug/libv8.so
#19 0x000023c775a81599 in ?? ()
#20 0x00002ef586d46f01 in ?? ()
#21 0x0000000600000000 in ?? ()
#22 0x000023c775a81669 in ?? ()
#23 0x00000f16ea38c9c9 in ?? ()
#24 0x00002ef586d60861 in ?? ()
#25 0x00002ef586d60861 in ?? ()
#26 0x00000f16ea38c9c9 in ?? ()
#27 0x00002ef586d46f01 in ?? ()
#28 0x000023c775a81599 in ?? ()
#29 0x0000005500000000 in ?? ()
#30 0x00002ef586d60a09 in ?? ()
#31 0x0000000000000000 in ?? ()
```

Comment 1 by [sheriffbot](#) on Thu, Apr 1, 2021, 4:08 AM EDT Project Member

Labels: external_security_report

Comment 2 by [ClusterFuzz](#) on Thu, Apr 1, 2021, 2:59 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5123019547410432>.

Comment 3 by [ClusterFuzz](#) on Thu, Apr 1, 2021, 5:59 PM EDT Project Member

Labels: OS-Linux OS-Mac

Comment 4 by [ClusterFuzz](#) on Thu, Apr 1, 2021, 11:06 PM EDT Project Member

Labels: FoundIn-89 FoundIn-90 Security_Impact-Stable

Detailed Report: <https://clusterfuzz.com/testcase?key=5123019547410432>

Fuzzer: None

Job Type: linux_asan_d8

Platform Id: linux

Crash Type: Invalid-free

Crash Address: 0x7f11d7abe930

Crash State:

icu_68::Locale::init

icu_68::Locale::canonicalize

v8::internal::CanonicalizeLanguageTag

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_d8&range=71299:71300

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5123019547410432

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/5123019547410432> -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/Yh3qCYFvHj6E5jz5> so we can improve.

Comment 5 by [ClusterFuzz](#) on Thu, Apr 1, 2021, 11:35 PM 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 Thu, Apr 1, 2021, 11:35 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: ftang@chromium.org

Labels: Test-Predator-Auto-Owner

Automatically assigning owner based on suspected regression changelist <https://chromium.googlesource.com/v8/v8/+/-/bfbc5c28b02b07b0679816f1a1f1cd701048014> ([intl])

Validate locale by LocaleBuilder).

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 [ClusterFuzz](#) on Wed, Apr 7, 2021, 2:29 PM EDT Project Member

Labels: OS-Windows

Comment 8 by [adetaylor@google.com](#) on Wed, Apr 14, 2021, 5:01 PM EDT Project Member

Please could you temporarily avoid including any .js test code in the CLs for this - speak to hablich@ with questions.

Comment 9 by [ftang@chromium.org](#) on Tue, Apr 20, 2021, 12:42 PM EDT Project Member

Status: Started (was: Assigned)

Comment 10 by [ftang@chromium.org](#) on Tue, Apr 20, 2021, 9:14 PM EDT Project Member

can be reproduce after 69-1 landing. Could be caused by <https://unicode-org.atlassian.net/browse/ICU-21587> trying <https://github.com/unicode-org/icu/pull/1698> next

Comment 11 by [ftang@chromium.org](#) on Tue, Apr 20, 2021, 9:15 PM EDT Project Member

Labels: Pri-1

Comment 12 by [ftang@chromium.org](#) on Tue, Apr 20, 2021, 9:25 PM EDT Project Member

yes, it is fixed by <https://github.com/unicode-org/icu/pull/1698>

Comment 13 by [ftang@chromium.org](#) on Tue, Apr 20, 2021, 9:33 PM EDT Project Member

Cc: js...@chromium.org syg@chromium.org jkummerow@chromium.org

Comment 14 by ftang@chromium.org on Tue, Apr 20, 2021, 9:37 PM EDT Project Member

Labels: Security_Severity-Medium

Google internal fuzzer found ICU problem for <https://unicode-org.atlassian.net/browse/ICU-21587> in March 27 2021 which trigger our work to fix it in <https://github.com/unicode-org/icu/pull/1698>

Comment 15 by ftang@chromium.org on Tue, Apr 20, 2021, 9:39 PM EDT Project Member

related google internal bugs are 182675373 182960178 183794356 183861617 183887128 which were filed March 13, March 16, March 26, March 27 and March 28 .

Comment 16 by sheriffbot on Wed, Apr 21, 2021, 1:02 PM EDT Project Member

Labels: M-90 Target-90

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

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

Comment 17 by Git Watcher on Wed, Apr 21, 2021, 6:43 PM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/deps/icu/+d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c>

commit d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c

Author: Frank Tang <ftang@chromium.org>

Date: Wed Apr 21 01:31:40 2021

Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>
<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

~~Bug-chromium:1104900~~

Change-Id: I39edcf04f43c52f6937365e50f521fab3679568b

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2842864>

Reviewed-by: Jungshik Shin <jshin@chromium.org>

[modify] <https://crrev.com/d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c/README.chromium>
[add] https://crrev.com/d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c/patches/locid_operators.patch
[modify] <https://crrev.com/d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c/source/common/locid.cpp>

Comment 18 by Git Watcher on Thu, Apr 22, 2021, 2:11 PM EDT Project Member

Labels: merge-merged-m90

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/deps/icu/+7e128ffcd0919c956962366c7347cf4633785339>

commit 7e128ffcd0919c956962366c7347cf4633785339

Author: Frank Tang <ftang@chromium.org>

Date: Wed Apr 21 01:31:40 2021

[m90] Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>
<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

~~Bug-chromium:1104900~~

Change-Id: I39edcf04f43c52f6937365e50f521fab3679568b

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2842864>

Reviewed-by: Jungshik Shin <jshin@chromium.org>

(cherry picked from commit d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2847140>

Reviewed-by: Frank Tang <ftang@chromium.org>

[modify] <https://crrev.com/7e128ffcd0919c956962366c7347cf4633785339/README.chromium>
[add] https://crrev.com/7e128ffcd0919c956962366c7347cf4633785339/patches/locid_operators.patch
[modify] <https://crrev.com/7e128ffcd0919c956962366c7347cf4633785339/source/common/locid.cpp>

Comment 19 by Git Watcher on Thu, Apr 22, 2021, 3:23 PM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+5846c2ac22f397073eeb818bf43a9c14756e5445>

commit 5846c2ac22f397073eeb818bf43a9c14756e5445

Author: Frank Tang <ftang@chromium.org>

Date: Thu Apr 22 19:22:07 2021

Roll ICU to fix crash

Upstream bug: <https://unicode-org.atlassian.net/browse/ICU-21587>
Upstream PR: <https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

<https://chromium.googlesource.com/chromium/deps/icu.git/+log/7e7574bd..d25bdc01>

Security team request NOT to include test in the CL.

~~Bug-chromium:1104900~~

Change-Id: I961e995a56fdb8181249558a536acc85f8980f60

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2846020>

Reviewed-by: Jungshik Shin <jshin@chromium.org>

Commit-Queue: Frank Tang <ftang@chromium.org>

Cr-Commit-Position: refs/heads/master@{#875299}

[modify] <https://crrev.com/5846c2ac22f397073eeb818bf43a9c14756e5445/DEPS>

Comment 20 by Git Watcher on Thu, Apr 22, 2021, 3:37 PM EDT Project Member

Labels: merge-merged-m91

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/deps/icu/+690d11b7d9856ef8cb712f93e65a2f11125511f1>

commit 690d11b7d9856ef8cb712f93e65a2f11125511f1

Author: Frank Tang <ftang@chromium.org>

Date: Wed Apr 21 01:31:40 2021

[m91] Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>
<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

~~Bug-chromium:1104490~~

Change-Id: I39edcf04f43c52f6937365e50f521fab3679568b
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2842864>
Reviewed-by: Jungshik Shin <jshin@chromium.org>
(cherry picked from commit d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c)
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2845799>
Reviewed-by: Frank Tang <ftang@chromium.org>

[modify] <https://crrev.com/690d11b7d9856ef8cb712f93e65a2f1125511f1/README.chromium>
[add] https://crrev.com/690d11b7d9856ef8cb712f93e65a2f1125511f1/patches/locid_operators.patch
[modify] <https://crrev.com/690d11b7d9856ef8cb712f93e65a2f1125511f1/source/common/locid.cpp>

Comment 21 by ftang@chromium.org on Thu, Apr 22, 2021, 4:22 PM EDT Project Member

Labels: -merge-merged-m90 -merge-merged-m91

Took out incorrect merged-merge labels. Nothing merge into m90 or m91 branch yet. These two are landed into branch prepare for m90 and m91 in the ICU branch. These were not yet merged into m90 or m91 yet

The real CLs to merge for m90 and m91 are

For m90 on refs/branch-heads/4430
<https://chromium-review.googlesource.com/c/chromium/src/+2847033>

For m91 on refs/branch-heads/4472
<https://chromium-review.googlesource.com/c/chromium/src/+2846077>

We are waiting for the trunk and daily get out and verify that before put up merge request labels

Comment 22 by ftang@chromium.org on Fri, Apr 23, 2021, 1:56 PM EDT Project Member

Fix verified in 92.0.4486.0

Comment 23 by ftang@chromium.org on Fri, Apr 23, 2021, 1:57 PM EDT Project Member

Labels: Merge-Request-90 Merge-Request-91

Comment 24 by ftang@chromium.org on Fri, Apr 23, 2021, 2:04 PM EDT Project Member

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>

YES

2. Links to the CLs you are requesting to merge.

For m90 on refs/branch-heads/4430
<https://chromium-review.googlesource.com/c/chromium/src/+2847033>

For m91 on refs/branch-heads/4472
<https://chromium-review.googlesource.com/c/chromium/src/+2846077>

3. Has the change landed and been verified on ToT?

YES Land on Thu, Apr 22, 2021, 12:23 PM PDT as
<https://chromium-review.googlesource.com/c/chromium/src/+2846020>

<https://chromium.googlesource.com/chromium/src/+5846c2ac22f397073eeb818bf43a9c14756e5445>

Security team request NOT to include test in the CL.

The test is

```
v1 = 'MZ-65537RUZ-65537RQZ-65537RvZ-65537RTZ-65537RdZ-65537RMZ-65537RJZ-65537ReZ-65537RpZ-65537R-Z-65537R2Z-65537R5Z-65537R6Z-65537R-2Z-65537RnZ-65537RuZ-65537RmZ';  
v2 = BigInt(1);  
v2.toLocaleString(v1);  
`
```

Copy and paste above and m90 and m91 will crash

Verify the fix in 92.0.4486.0 Won't crash

4. Does this change need to be merged into other active release branches (M-1, M+1)?

Both m91 and m90

5. Why are these changes required in this milestone after branch?

Security issue

6. Is this a new feature?

NO

7. If it is a new feature, is it behind a flag using finch?

N/A

Comment 25 by srinivassista@google.com on Fri, Apr 23, 2021, 2:10 PM EDT Project Member

Cc: adetaylor@chromium.org

+adetaylor@ to review

Comment 26 by adetaylor@google.com on Fri, Apr 23, 2021, 2:34 PM EDT Project Member

Labels: -Merge-Request-91 Merge-Approved-91

Approving merge to M91, branch 4472. We should wait for more bake time before merging to M90.

Please mark as fixed: <https://chromium.googlesource.com/chromium/src/+master/docs/security/security-labels.md#TOC-Merge-labels>

Comment 27 by ftang@chromium.org on Fri, Apr 23, 2021, 2:59 PM EDT Project Member

Status: Fixed (was: Started)

Comment 28 by [Git Watcher](#) on Fri, Apr 23, 2021, 5:42 PM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+3d9c4b0096b88097e16576f8d8b7617ea9e8219f>

commit [3d9c4b0096b88097e16576f8d8b7617ea9e8219f](#)

Author: Frank Tang <ftang@chromium.org>

Date: Fri Apr 23 21:41:12 2021

[m91] Roll ICU to Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>

<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

<https://chromium.googlesource.com/chromium/deps/icu.git/+log/81d6568..690d11b7>

~~Bug: chromium:1104890~~

Change-Id: [I670b1f69d677776beef74e54d1931f7543b08a7](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2846077>

Reviewed-by: Jungshik Shin <jshin@chromium.org>

Commit-Queue: Frank Tang <ftang@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#370}

Cr-Branched-From: [3d60439cfb36485e76a1c5bb7f513d3721b20da1](#)-refs/heads/master@{#870763}

[modify] <https://crrev.com/3d9c4b0096b88097e16576f8d8b7617ea9e8219f/DEPS>

Comment 29 by [sheriffbot](#) on Sat, Apr 24, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 30 by [sheriffbot](#) on Sat, Apr 24, 2021, 2:01 PM EDT Project Member

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

Comment 31 by [ClusterFuzz](#) on Tue, Apr 27, 2021, 10:33 AM EDT Project Member

Status: Verified (was: Fixed)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5123019547410432 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_d8&range=74190:74191

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

Comment 32 by amyressler@google.com on Wed, Apr 28, 2021, 7:24 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 33 by ftang@chromium.org on Wed, Apr 28, 2021, 7:28 PM EDT Project Member

Somehow the test case is still crashed in 91.0.4472.27

Could be caused by some other bug fixed in icu 69-1 (m91 is on 68-1)

Comment 34 by amyressler@google.com on Fri, Apr 30, 2021, 1:51 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 35 by adetaylor@google.com on Mon, May 3, 2021, 11:28 AM EDT Project Member

Status: Assigned (was: Verified)

ftang@ please could you look into #c33?

Comment 36 by adetaylor@google.com on Mon, May 3, 2021, 11:29 AM EDT Project Member

(I realize now, of course, that you actually _made_ [comment 33](#)! But either way, it seems the bug should be Assigned not Verified. Thanks!)

Comment 37 by ftang@chromium.org on Wed, May 5, 2021, 1:27 AM EDT Project Member

It is fixed and verify in m92, which is based on ICU 69.

After I apply the PR to m91, which is based on ICU 68, the cp PR is not enough to fix the crash.

Comment 38 by adetaylor@chromium.org on Wed, May 5, 2021, 12:01 PM EDT Project Member

OK. Do you think it would be easy to identify what fixed this in ICU 69? If so, please do that, so we can consider merging the fix back to M91 and maybe M90. However, if it's hard to identify the specific fix, then maybe this can wait to be fixed in M92.

Comment 39 by ftang@chromium.org on Wed, May 5, 2021, 6:19 PM EDT Project Member

The root cause is somehow we didn't cp <https://github.com/unicode-org/icu/pull/1656/files> into m90 or m91.

Comment 40 by ftang@chromium.org on Wed, May 5, 2021, 6:42 PM EDT Project Member

Labels: Merge-Request-91

fix for m91 in <https://chromium-review.googlesource.com/c/chromium/src/+2874872>

Comment 41 by [sheriffbot](#) on Wed, May 5, 2021, 6:47 PM EDT Project Member

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: DEPS changes referenced in bugdroid comments.

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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?

5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:

8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: <http://go/cros-engprodcomponents>

Please contact the milestone owner if you have questions.

Owners: benmason@(Android), bindusuvama@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 42 by ftang@chromium.org on Wed, May 5, 2021, 6:50 PM EDT Project Member

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>

YES

2. Links to the CLs you are requesting to merge.

For m91 on refs/branch-heads/4472

<https://chromium-review.googlesource.com/c/chromium/src/+2874872>

3. Has the change landed and been verified on ToT?

It was already part of trunk for a while. Came with ICU69-1

Security team request NOT to include test in the CL.

The test is

```
,  
  
v1 = 'MZ-65537RUZ-65537RQZ-65537RvZ-65537RTZ-65537RdZ-65537RMZ-65537RJZ-65537ReZ-65537RpZ-65537R-Z-65537R2Z-65537R5Z-65537R6Z-65537R-2Z-65537RnZ-65537RuZ-65537RmZ';  
v2 = BigInt(1);  
v2.toLocaleString(v1);  
,
```

Copy and paste above and m90 and m91 will crash

Verify the fix in 92.0.4486.0 Won't crash

4. Does this change need to be merged into other active release branches (M-1, M+1)?

Both m91 and m90

5. Why are these changes required in this milestone after branch?

Security issue

6. Is this a new feature?

NO

7. If it is a new feature, is it behind a flag using finch?

N/A

Comment 43 by adetaylor@google.com on Thu, May 6, 2021, 12:48 PM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Discussed with ftang yesterday - approving merge of the other half of the fix to M91, branch 4472.

Comment 44 by [Git Watcher](#) on Thu, May 6, 2021, 9:16 PM EDT Project Member

Labels: -merge-approved-91

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+b3e7d3bc1c8850e1fab5adb5f095a1c163870579>

commit b3e7d3bc1c8850e1fab5adb5f095a1c163870579

Author: Frank Tang <ftang@chromium.org>

Date: Fri May 07 01:15:35 2021

[m91] Roll ICU w/ fix of invalid free by long locale name

<https://chromium.googlesource.com/chromium/deps/icu.git/+log/690d11b7..6266caed>

~~Bug=1404800~~

Change-Id: Ic929c7ea72c9cde45c240dd1913a0963be44468f

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2874872>

Reviewed-by: Frank Tang <ftang@chromium.org>

Reviewed-by: Jungshik Shin <jshin@chromium.org>

Commit-Queue: Frank Tang <ftang@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#816}

Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] <https://crrev.com/b3e7d3bc1c8850e1fab5adb5f095a1c163870579/DEPS>

Comment 45 by ftang@chromium.org on Fri, May 7, 2021, 1:19 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 46 by ftang@chromium.org on Wed, May 12, 2021, 5:45 PM EDT Project Member

Verified on Version 91.0.4472.57 (Official Build) beta (x86_64)

Comment 47 by adetaylor@google.com on Fri, May 21, 2021, 3:43 PM EDT Project Member

Labels: -Merge-Request-90

Comment 48 by amyressler@chromium.org on Mon, May 24, 2021, 11:11 AM EDT Project Member

Labels: Release-0-M91

Comment 49 by amyressler@google.com on Mon, May 24, 2021, 2:19 PM EDT Project Member

Labels: CVE-2021-30535 CVE_description-missing

Comment 50 by wxmp...@gmail.com on Tue, May 25, 2021, 9:44 AM EDT
Thanks! Please credit to leogan, nocma, cheneyxu of WeChat Open Platform Security Team.

Comment 51 by janag...@google.com on Wed, May 26, 2021, 9:32 AM EDT Project Member
Cc: janag...@google.com
Labels: LTS-Security-86

Comment 52 by janag...@google.com on Thu, May 27, 2021, 9:18 AM EDT Project Member
Labels: LTS-Merge-Request-86

Comment 53 by sheriffbot on Thu, May 27, 2021, 12:21 PM EDT Project Member
Labels: -M-90 M-91 Target-91

Comment 54 by Git Watcher on Thu, May 27, 2021, 10:17 PM EDT Project Member
Labels: merge-merged-m86

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/deps/icu/+95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f>

commit 95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f
Author: Frank Tang <ftang@chromium.org>
Date: Wed Apr 21 01:31:40 2021

[86-LTS] Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>
<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

~~Bug-chromium:1404890~~

Change-Id: I39edcf04f43c52f6937365e50f521fab3679568b
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2842864>
Reviewed-by: Jungshik Shin <jshin@chromium.org>
(cherry picked from commit d25bdc013cb0d0d9b1b7c53beb1ab2a30323341c)
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/deps/icu/+2919701>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Frank Tang <ftang@chromium.org>

[modify] <https://crrev.com/95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f/README.chromium>
[add] https://crrev.com/95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f/patches/locid_operators.patch
[modify] <https://crrev.com/95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f/source/common/locid.cpp>

Comment 55 by Git Watcher on Mon, May 31, 2021, 11:38 AM EDT Project Member
Labels: merge-merged-4240

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+4174427c03fbbea4191306641d8786f9344806e3>

commit 4174427c03fbbea4191306641d8786f9344806e3
Author: Jana Grill <janagrill@google.com>
Date: Mon May 31 15:37:23 2021

[86-LTS] Roll ICU to fix crash

Upstream bug: <https://unicode-org.atlassian.net/browse/ICU-21587>
Upstream PR: <https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

<https://chromium.googlesource.com/chromium/deps/icu.git/+95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f>

~~Bug-chromium:1404890~~

Change-Id: Ie8429bdf8b68e2ec92fdcfca06e161db707ccb2
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2925595>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Jana Grill <janagrill@google.com>
Cr-Commit-Position: refs/branch-heads/4240@(#1653)
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@(#800218)

[modify] <https://crrev.com/4174427c03fbbea4191306641d8786f9344806e3/DEPS>

Comment 56 by Git Watcher on Tue, Jun 1, 2021, 2:39 AM EDT Project Member
The following revision refers to this bug:
<https://webrtc.googlesource.com/src/+6b79468a0cb1d99d0e684e590053b57441145d75>

commit 6b79468a0cb1d99d0e684e590053b57441145d75
Author: Mirko Bonadei <mbonadei@webrtc.org>
Date: Mon May 31 14:47:46 2021

[Merge M86] Roll ICU to fix crash

Upstream bug: <https://unicode-org.atlassian.net/browse/ICU-21587>
Upstream PR: <https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

<https://chromium.googlesource.com/chromium/deps/icu.git/+95e145fcc72edac4cb1f31c7d1816b2e46eeeb6f>

TBR=titovartem@webrtc.org

No-Try: True
No-PreSubmit: True

~~Bug-chromium:1404890~~

Change-Id: I1258a4c90fd7e6a7dee18459fa91b0e2ce258c16
Reviewed-on: <https://webrtc-review.googlesource.com/c/src/+220924>
Reviewed-by: Mirko Bonadei <mbonadei@webrtc.org>
Reviewed-by: Artem Titov <titovartem@webrtc.org>
Commit-Queue: Mirko Bonadei <mbonadei@webrtc.org>
Cr-Commit-Position: refs/branch-heads/4240@(#20)
Cr-Branched-From: 93a9d19d4eb53b3f4fb4d22e6c54f2e2824437eb-refs/heads/master@(#31969)

[modify] <https://crrev.com/6b79468a0cb1d99d0e684e590053b57441145d75/DEPS>

Comment 57 by Git Watcher on Tue, Jun 1, 2021, 3:38 AM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+391e5a0a0c0bc1cbde7aa886c553210605e8d7e6>

commit 391e5a0a0c0bc1cbde7aa886c553210605e8d7e6
Author: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Date: Tue Jun 01 07:37:04 2021

Roll WebRTC from 1627015c8408 to 6b79468a0cb1 (1 revision)

<https://webrtc.googlesource.com/src.git/+log/1627015c8408..6b79468a0cb1>

2021-06-01 mbonadei@webrtc.org [Merge M86] Roll ICU to fix crash

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
<https://autoroll.skia.org/r/webrtc-chromium-lts>
Please CC cros-lts-team@google.com on the revert to ensure that a human
is aware of the problem.

To report a problem with the AutoRoller itself, please file a bug:
<https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug>

Documentation for the AutoRoller is here:
<https://skia.googlesource.com/buildbot/+doc/master/autoroll/README.md>

~~Bug-chromium:1104900~~
Tbr: cros-lts-team@google.com
Change-Id: Ie498aa26d25e6e3930f92f8508c5f9fbdadbc5ce
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2929896>
Commit-Queue: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Bot-Commit: Chrome Release Autoroll <chromium-release-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1654}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] <https://crrev.com/391e5a0a0c0bc1cbde7aa886c553210605e8d7e6/DEPS>

Comment 58 by janag...@google.com on Tue, Jun 1, 2021, 5:50 AM EDT Project Member
Labels: -LTS-Merge-Request-86 LTR-Merged-86

Comment 59 by surabhigrover@google.com on Tue, Jun 1, 2021, 10:26 AM EDT Project Member
Labels: LTS-Merge-Approved-86

Comment 60 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 61 by vsavu@google.com on Mon, Jun 14, 2021, 12:42 PM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 62 by gianluca@google.com on Tue, Jun 15, 2021, 6:29 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 63 by [Git Watcher](#) on Tue, Jun 15, 2021, 12:41 PM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+b0fa78c8430045c8126c7552c4d0bc9559a5ed66>

commit b0fa78c8430045c8126c7552c4d0bc9559a5ed66
Author: Frank Tang <ftang@chromium.org>
Date: Tue Jun 15 16:40:25 2021

[m90] Roll ICU to Fix crash caused by locale assign/move operators

<https://unicode-org.atlassian.net/browse/ICU-21587>
<https://bugs.chromium.org/p/chromium/issues/detail?id=1194899>

<https://chromium.googlesource.com/chromium/deps/icu.git/+log/e05b663d..7e128ffc>

~~Bug-chromium:1104900~~
Change-Id: I15f0bea5be7161c97832ba45de6b513351c5be3d
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2847033>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuth@chromium.org>
Commit-Queue: Frank Tang <ftang@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1524}
Cr-Branched-From: e5ce7dc47518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] <https://crrev.com/b0fa78c8430045c8126c7552c4d0bc9559a5ed66/DEPS>

Comment 64 by janag...@google.com on Wed, Jul 28, 2021, 5:23 AM EDT Project Member
Labels: -LTS-Merge-Approved-86 -LTS-Merge-Approved-90 LTS-Merged-90

Comment 65 by [sheriffbot](#) on Tue, Sep 21, 2021, 1:31 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