Starred by 5 users

Owner: ishell@chromium.org

CC: adetaylor@chromium.org
pbomm...@chromium.org
ishell@chromium.org
gmpritchard@google.com
amyressler@chromium.org
danno@chromium.org
vahl@chromium.org
leszeks@chromium.org
verwa...@chromium.org
ecmziegler@google.com

Status: Fixed *(Closed)*

Components: Blink>JavaScript>Runtime

Modified: Aug 5, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

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

Pri: 1

Type: Bug-Security

M-100
Security_Severity-High
ReleaseBlock-Stable
allpublic
CVE_description-submitted
Target-100
FoundIn-100
M-101
Target-101
Security_Impact-Extended
merge-merged-9.6
V8-postmortem
LTS-Merge-Merged-96
merge-merged-10.0
merge-merged-10.1
merge-merged-4978
Release-1-M100

CVE-2022-1232
V8-postmortem-obsolete

Issue 1311641: Security: Incomplete fix for CVE-2022-1096

Reported by glazunov@google.com on Wed, Mar 30, 2022, 9:16 AM EDT Project Member

Code

VULNERABILITY DETAILS

The fix for https://crbug.com/1309225 has modified `SetPropertyInternal()` to fall back to `SetSuperProperty()` whenever a property access interceptor is encountered because `SetSuperProperty()` is robust against possible side effects caused by interceptors.

Unfortunately, the function `JSObject::DefineOwnPropertyIgnoreAttributes()` is also affected by the bug and requires the same change.

VERSION

Google Chrome 100.0.4896.60 (Official Build) (arm64)
Chromium 102.0.4972.0 (Developer Build) (64-bit)

REPRODUCTION CASE

To make the exploit functional again, the attacker only needs to replace one property store with an `Object.defineProperty()` call:

```
<script>
style = document.createElement('p').style;
Object.defineProperty(style, 'prop', {
  value: { toString() { style.prop = 1 } }
});
</script>
```

The repro case above triggers the same DCHECK failure:

```
#
# Fatal error in ../../v8/src/objects/map.cc, line 437
# Debug check failed: map->instance_descriptors(isolate) .Search(*name, map->NumberOfOwnDescriptors())
.is_not_found().
#
```

CREDIT INFORMATION

Sergei Glazunov of Google Project Zero

This bug is subject to a 90-day disclosure deadline. If a fix for this
issue is made available to users before the end of the 90-day deadline,

this bug report will become public 30 days after the fix was made
available. Otherwise, this bug report will become public at the deadline.
The scheduled deadline is 2022-06-28

The scheduled deadline is 2022-06-28.

Comment 1 by ishell@chromium.org on Wed, Mar 30, 2022, 9:43 AM EDT Project Member

Status: Started (was: Unconfirmed)
Owner: ishell@chromium.org
Components: Blink>JavaScript>Runtime

Comment 2 by ClusterFuzz on Wed, Mar 30, 2022, 3:18 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5132813107789824.

Comment 3 by glazunov@google.com on Thu, Mar 31, 2022, 5:23 AM EDT Project Member

Cc: adetaylor@chromium.org amyressler@chromium.org

Since the original bug wasn't reported by Project Zero, we can't apply the shortened deadline for variants under our current disclosure policy. Nevertheless, please consider releasing the patch to the users ASAP. The threat actor is most likely aware of the fact that the fix is incomplete. Additionally, the original issue is getting attention on Twitter, so we expect that other researchers will likely re-discover the variant soon.

Comment 4 by amyressler@chromium.org on Thu, Mar 31, 2022, 12:00 PM EDT Project Member

Labels: Security_Severity-High FoundIn-100 OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-0

Thanks for the heads-up, Sergei. I concur that we should get this patched and the fix out to users as soon as possible given the existing active exploit could be easily updated the threat actor and they would have seen our existing patch already in the emergency release. Igor is actively working on a fix.

Severity High -- as this allows for renderer RCE
Pri-0 -- a weponized exploit exists for a close variant of this issue
FoundIn-100 -- 100 is now Stable channel and will be new extended stable, issue exists prior

Comment 5 by sheriffbot on Thu, Mar 31, 2022, 12:05 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 6 by sheriffbot on Thu, Mar 31, 2022, 12:47 PM EDT Project Member

Labels: M-100 Target-100

Setting milestone and target because of high severity.

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

Comment 7 by gmpritchard@google.com on Thu, Mar 31, 2022, 12:59 PM EDT Project Member

Cc: gmpritchard@google.com

Comment 8 by gov...@chromium.org on Thu, Mar 31, 2022, 1:01 PM EDT Project Member

Labels: M-101 Target-101 ReleaseBlock-Stable

Comment 9 by sheriffbot on Thu, Mar 31, 2022, 1:07 PM EDT Project Member

Labels: -Pri-0 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 Git Watcher on Fri, Apr 1, 2022, 6:37 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49

commit c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49
Author: Igor Sheludko <ishell@chromium.org>
Date: Thu Mar 31 21:47:27 2022

[runtime] Fix handling of interceptors, pt.3

... in JSObject::DefineOwnPropertyIgnoreAttributes().
Don't execute interceptor again if it declined to handle the operation.

~~Bug: chromium:1311641~~
Change-Id: If61ed40665ff7d81e96fa6bf29bbb5dfbeadfcc1
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3562979
Reviewed-by: Toon Verwaest <verwaest@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79707}

[modify] https://crrev.com/c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49/src/objects/js-objects.cc
[modify] https://crrev.com/c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49/test/cctest/test-api-interceptors.cc

Comment 11 by ishell@chromium.org on Fri, Apr 1, 2022, 6:40 AM EDT Project Member

Status: Fixed (was: Started)

Comment 12 by amyressler@chromium.org on Fri, Apr 1, 2022, 11:15 AM EDT Project Member

Labels: Merge-Request-101 Merge-Request-100

Pre-empting the bot and adding merge request labels to M101 and M100.

Comment 13 by Git Watcher on Fri, Apr 1, 2022, 11:19 AM EDT Project Member

Labels: merge-merged-4978

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/9c9c8cc00c3f8e2531c532a4b37d178a477bbc5d

commit 9c9c8cc00c3f8e2531c532a4b37d178a477bbc5d
Author: Igor Sheludko <ishell@chromium.org>
Date: Thu Mar 31 21:47:27 2022

[runtime] Fix handling of interceptors, pt.3

... in JSObject::DefineOwnPropertyIgnoreAttributes().

Don't execute interceptor again if it declined to handle the operation.

Bug: chromium:1311641

~~Bug: chromium:1311641~~
Change-Id: If61ed40665ff7d81e96fa6bf29bbb5dfbeadfcc1
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3562979
Reviewed-by: Toon Verwaest <verwaest@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/heads/main@{#79707}
(cherry picked from commit c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49)
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3565845
Reviewed-by: Igor Sheludko <ishell@chromium.org>

[modify] https://crrev.com/9c9c8cc00c3f8e2531c532a4b37d178a477bbc5d/src/objects/js-objects.cc
[modify] https://crrev.com/9c9c8cc00c3f8e2531c532a4b37d178a477bbc5d/test/cctest/test-api-interceptors.cc

Comment 14 by sheriffbot on Fri, Apr 1, 2022, 11:19 AM EDT Project Member

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 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 15 by Git Watcher on Fri, Apr 1, 2022, 12:34 PM EDT Project Member

Labels: merge-merged-10.1

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/07e7c60fdb533f6069ec1479bfa06b7333165d5d

commit 07e7c60fdb533f6069ec1479bfa06b7333165d5d
Author: Igor Sheludko <ishell@chromium.org>
Date: Fri Apr 01 15:33:10 2022

Merged: [runtime] Fix handling of interceptors, pt.3

... in JSObject::DefineOwnPropertyIgnoreAttributes().
Don't execute interceptor again if it declined to handle the operation.

~~Bug: chromium:1311641~~
(cherry picked from commit c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49)

Change-Id: I20e417ae5c76287f447971aff18f622c36fc2f1b
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3564571
Reviewed-by: Toon Verwaest <verwaest@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.1@{#10}
Cr-Branched-From: b003970395b7efcc309eb30b4ca06dd8385acd55-refs/heads/10.1.124@{#1}
Cr-Branched-From: e62f556862624103ea1da5b9dcef9b216832033b-refs/heads/main@{#79503}

[modify] https://crrev.com/07e7c60fdb533f6069ec1479bfa06b7333165d5d/src/objects/js-objects.cc
[modify] https://crrev.com/07e7c60fdb533f6069ec1479bfa06b7333165d5d/test/cctest/test-api-interceptors.cc

[modify] https://crrev.com/07e7c60fdb533f6b69ec1479bfa06b73331b5d5d/test/cctest/test-api-interceptors.cc

Comment 16 by Git Watcher on Fri, Apr 1, 2022, 12:35 PM EDT Project Member

Labels: merge-merged-10.0

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/36b66b5cc99147edc594a69f4b94f7828fc94750

commit 36b66b5cc99147edc594a69f4b94f7828fc94750
Author: Igor Sheludko <ishell@chromium.org>
Date: Fri Apr 01 15:41:24 2022

Merged: [runtime] Fix handling of interceptors, pt.3

... in JSObject::DefineOwnPropertyIgnoreAttributes().
Don't execute interceptor again if it declined to handle the operation.

~~Bug: chromium:1311641~~
(cherry picked from commit c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49)

Change-Id: Ie9aef5a98959403f6a26e6bef7f4a77d312bd62a
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3563560
Reviewed-by: Toon Verwaest <verwaest@chromium.org>
Cr-Commit-Position: refs/branch-heads/10.0@{#16}
Cr-Branched-From: 6ea73a738c467dc26abbbe84e27a36aac1c6e119-refs/heads/10.0.139@{#1}
Cr-Branched-From: ccc689011280419901e6ee42cae39980c0e96030-refs/heads/main@{#79131}

[modify] https://crrev.com/36b66b5cc99147edc594a69f4b94f7828fc94750/src/objects/js-objects.cc
[modify] https://crrev.com/36b66b5cc99147edc594a69f4b94f7828fc94750/test/cctest/test-api-interceptors.cc

Comment 17 by gov...@chromium.org on Fri, Apr 1, 2022, 1:00 PM EDT Project Member

Labels: -Merge-Request-100 -Merge-Request-101

Comment 18 by sheriffbot on Fri, Apr 1, 2022, 1:40 PM EDT Project Member

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

Comment 19 by sheriffbot on Mon, Apr 4, 2022, 3:35 AM EDT Project Member

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=1311641&entry.364066060=Internal&entry.958145677=Android&entry.958145677=Chrome&entry.958145677=Fuchsia&entry.958145677=Linux&entry.958145677=Mac&entry.958145677=Windows&entry.958145677=Lacros&entry.763880440=Extended&entry.1678852700=High&entry.763402679=Blink>JavaScript>Runtime&entry.975983575=ishell@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 20 by vahl@chromium.org on Mon, Apr 4, 2022, 5:10 AM EDT Project Member

Cc: danno@chromium.org

Comment 21 by vahl@chromium.org on Mon, Apr 4, 2022, 5:18 AM EDT Project Member

Cc: pbomm...@chromium.org

@Release TPMs.
The initial fix was merged to M99 as well [1], but as M100 is the current stable IMO this is not needed. PLMK in case we should prep the merge to M99 as well.

[1] https://bugs.chromium.org/p/chromium/issues/detail?id=1309225#c30

Comment 22 by voit@google.com on Mon, Apr 4, 2022, 7:58 AM EDT Project Member

Labels: LTS-Evaluating-96

Comment 23 by voit@google.com on Mon, Apr 4, 2022, 8:53 AM EDT Project Member

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

Comment 24 by Git Watcher on Mon, Apr 4, 2022, 8:56 AM EDT Project Member

Labels: merge-merged-9.6

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/f599381978f2f9463afdb154146ad210e89dad0a

commit f599381978f2f9463afdb154146ad210e89dad0a
Author: Igor Sheludko <ishell@chromium.org>
Date: Mon Apr 04 12:42:56 2022

[M96-LTS][runtime] Fix handling of interceptors, pt.3

... in JSObject::DefineOwnPropertyIgnoreAttributes().
Don't execute interceptor again if it declined to handle the operation.

(cherry picked from commit c4e66b89b4ecd0e90b31e9e4ed08d38085a84c49)

~~Bug: chromium:1311641~~
No-Try: true
No-Presubmit: true
No-Tree-Checks: true
Change-Id: Ie9aef5a98959403f6a26e6bef7f4a77d312bd62a
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3568921
Reviewed-by: Lutz Vahl <vahl@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Commit-Queue: Igor Sheludko <ishell@chromium.org>
Cr-Commit-Position: refs/branch-heads/9.6@{#56}
Cr-Branched-From: 0b7bda016178bf438f09b3c93da572ae3663a1f7-refs/heads/9.6.180@{#1}
Cr-Branched-From: 41a5a247d9430b953e38631e88d17790306f7a4c-refs/heads/main@{#77244}

[modify] https://crrev.com/f599381978f2f9463afdb154146ad210e89dad0a/src/objects/js-objects.cc
[modify] https://crrev.com/f599381978f2f9463afdb154146ad210e89dad0a/test/cctest/test-api-interceptors.cc

Comment 25 by sheriffbot on Mon, Apr 4, 2022, 9:00 AM EDT Project Member

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 26 by gmpritchard@google.com on Mon, Apr 4, 2022, 9:02 AM EDT Project Member

Labels: -LTS-Merge-Candidate -merge-merged-10.0 LTS-Merge-Approved-96

Comment 27 by ishell@chromium.org on Mon, Apr 4, 2022, 9:19 AM EDT Project Member

Answering to #c25.

1. One CL: https://chromium-review.googlesource.com/c/v8/v8/+/3562979
2. Simple (major part of the CL is a regression test)
3. Yes, it was merged to M100.
4. Yes.

Comment 28 by gmpritchard@google.com on Mon, Apr 4, 2022, 11:35 AM EDT Project Member

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

Comment 29 by sheriffbot on Mon, Apr 4, 2022, 2:52 PM EDT Project Member

Labels: Merge-TBD-100

This release blocking issue appears to be targeted for one or more milestones which may have already branched:

- M100, which branched on 2022-02-17 (Chromium branch: 4896, Chromium branch position: 972766)

Because this issue was marked as fixed on or after branch day, a merge of any CLs which landed on or after branch day may be required.

If no merge is needed (e.g. the necessary CLs are already present in the relevant branch), please remove the Merge-TBD-## label and replace it with a Merge-NA-## label (where ## corresponds to the milestone under evaluation). If a merge is necessary, please add the appropriate Merge-Request-## labels. If you're not sure, reach out to the relevant release manager (can be found at https://chromiumdash.appspot.com/schedule).

To learn more about the merge process, including how to land any required merges, see https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md.

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

Comment 30 by amyressler@chromium.org on Mon, Apr 4, 2022, 2:53 PM EDT Project Member

Labels: -Merge-TBD-100

already merged to M100

Comment 31 by amyressler@chromium.org on Mon, Apr 4, 2022, 3:17 PM EDT Project Member

Labels: Release-1-M100

Comment 32 by amyressler@google.com on Mon, Apr 4, 2022, 3:20 PM EDT Project Member

Labels: CVE-2022-1232 CVE_description-missing

Comment 33 by sheriffbot on Tue, Apr 5, 2022, 2:53 PM EDT Project Member

Labels: Merge-TBD-100

This release blocking issue appears to be targeted for one or more milestones which may have already branched:

- M100, which branched on 2022-02-17 (Chromium branch: 4896, Chromium branch position: 972766)

Because this issue was marked as fixed on or after branch day, a merge of any CLs which landed on or after branch day may be required.

If no merge is needed (e.g. the necessary CLs are already present in the relevant branch), please remove the Merge-TBD-## label and replace it with a Merge-NA-## label (where ## corresponds to the milestone under evaluation). If a merge is necessary, please add the appropriate Merge-Request-## labels. If you're not sure, reach out to the relevant release manager (can be found at https://chromiumdash.appspot.com/schedule).

To learn more about the merge process, including how to land any required merges, see https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md.

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

Comment 34 by amyressler@chromium.org on Tue, Apr 5, 2022, 3:19 PM EDT Project Member

Labels: -Merge-TBD-100 merge-merged-10.0

adding back the merge label for 10.0-lkgr and cease fighting with the bot over the tbd label as this was merged to m100

Comment 35 by ishell@chromium.org on Tue, May 24, 2022, 8:55 AM EDT Project Member

Labels: V8-postmortem-obsolete

The postmortem for this issue is the same as for https://crbug.com/1309225.

Comment 36 by sheriffbot on Fri, Jul 8, 2022, 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

Comment 37 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 38 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

Comment 39 by Git Watcher on Fri, Aug 5, 2022, 2:07 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/v8/v8/+/3c7f274770e90b766ed554a6ca599e70341c9735

commit 3c7f274770e90b766ed554a6ca599e70341c9735
Author: Brendon Tiszka <tiszka@chromium.org>
Date: Thu Aug 04 18:46:33 2022

[runtime] Add runtime checks for name collisions

~~Bug: chromium:1216437~~,~~chromium:1219630~~,chromium:1309225
~~Bug: chromium:1311641~~,~~chromium:1314616~~
Change-Id: I1575edbdd7fe91ed970ffe2f3437fd7c514e1ebd
Reviewed-on: https://chromium-review.googlesource.com/c/v8/v8/+/3794525
Reviewed-by: Samuel Groß <saelo@chromium.org>
Reviewed-by: Igor Sheludko <ishell@chromium.org>
Commit-Queue: Brendon Tiszka <tiszka@chromium.org>
Cr-Commit-Position: refs/heads/main@{#82235}

[modify] https://crrev.com/3c7f274770e90b766ed554a6ca599e70341c9735/test/unittests/objects/object-unittest.cc
[modify] https://crrev.com/3c7f274770e90b766ed554a6ca599e70341c9735/src/objects/descriptor-array.h
[modify] https://crrev.com/3c7f274770e90b766ed554a6ca599e70341c9735/src/objects/descriptor-array-inl.h
[modify] https://crrev.com/3c7f274770e90b766ed554a6ca599e70341c9735/src/objects/objects.cc
[modify] https://crrev.com/3c7f274770e90b766ed554a6ca599e70341c9735/src/objects/objects.h