Starred by 2 users

Owner:	gman@chromium.org **Last visit 24 days ago**
CC:	kbr@chromium.org rzanoni@google.com cwallez@chromium.org enga@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebGL
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
M-100
Security_Severity-High
allpublic
CVE_description-submitted
Target-99
Target-100
FoundIn-99
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Merge-NA-102
Release-0-M101
CVE-2022-1482

Issue 1304987: clang-analyzer-core.uninitialized.Branch in third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc

Reported by diehl...@microsoft.com on Wed, Mar 9, 2022, 7:13 PM EST Project Member

Code

Description #2 by diehl...@microsoft.com (Mar 9, 2022)

Chrome Version: trun

File: third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc
Error: clang-analyzer-core.uninitialized.Branch

Diagnostics:

Line Number: 4002
Message: Branch condition evaluates to a garbage value


```
[
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3987,
  message: "'source_data_format' is not equal to kDataFormatNumFormats"
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3987,
  message: 'Taking false branch'
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3992,
  message: "Calling 'WebGLImageConversion::ComputeFormatAndTypeParameters'"
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3527,
  message: "Control jumps to 'case 6408:' at line 3546"
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3551,
  message: ' Execution continues on line 3555'

 },
 {
```

```
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3555,
  message: "Control jumps to 'case 33640:' at line 3583"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3586,
  message: ' Execution continues on line 3597'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3597,
  message: 'Returning the value 1, which participates in a condition later'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3992,
  message: "Returning from 'WebGLImageConversion::ComputeFormatAndTypeParameters'"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3992,
  message: 'Taking false branch'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3998,
  message: "'skip_size_in_bytes' declared without an initial value"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3999,
  message: "Calling 'WebGLImageConversion::ComputeImageSizeInBytes'"
},
{
  expansion_locs: [ [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3610,
  message: "'?' condition is true"
},
{
  expansion_locs: [ [Object], [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,

  message: "Assuming field 'alignment' is not equal to 1"
},
{
```

```
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [ [Object], [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,
  message: "Assuming field 'alignment' is not equal to 2"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [ [Object], [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3612,
  message: "Assuming field 'alignment' is not equal to 4"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [ [Object], [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3612,
  message: "Assuming field 'alignment' is equal to 8"
},
{
  expansion_locs: [ [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3611,
  message: "'?' condition is true"
},
{
  expansion_locs: [ [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3613,
  message: "Control jumps to 'case 0:' at line 3613"
},
{
  expansion_locs: [ [Object], [Object] ],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',

  line_number: 3613,
  message: 'Taking true branch'
}
```

},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3614,
  message: "Control jumps to 'case 0:' at line 3614"
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3614,
  message: 'Taking true branch'
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3615,
  message: "Control jumps to 'case 0:' at line 3615"
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3615,
  message: 'Taking true branch'
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3616,
  message: "Control jumps to 'case 0:' at line 3616"
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3616,
  message: 'Taking true branch'
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3617,
  message: "Control jumps to 'case 0:' at line 3617"
},
{
  expansion_locs: [[Object], [Object]],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3617,
  message: 'Taking true branch'
},
{
  expansion_locs: [],

  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: "'width' is >= 0"

```
  message:   'width' is >= 0
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: "'height' is >= 0"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: "'depth' is >= 0"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3618,
  message: 'Taking false branch'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620,
  message: "Assuming 'width' is not equal to 0"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620,
  message: "Assuming 'height' is not equal to 0"
},
{

  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620
```

```
  line_number: 3620,
  message: "Left side of '||' is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620,
  message: "'depth' is 1"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3620,
  message: 'Taking false branch'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3629,
  message: "Assuming field 'row_length' is <= 0"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3629,
  message: "'?' condition is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3630,
  message: "Assuming field 'image_height' is <= 0"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3630,
  message: "'?' condition is false"
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3633,
  message: 'Taking false branch'
},
{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3640,
  message: 'Taking true branch'
},

{
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
```

```
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3641,
  message: "Returning without writing to '*skip_size_in_bytes'"
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 3999,
  message: "Returning from 'WebGLImageConversion::ComputeImageSizeInBytes'"
 },
 {
  expansion_locs: [],
  file_path: 'third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc',
  line_number: 4002,
  message: 'Branch condition evaluates to a garbage value'
 }
]
```

```cpp
 const uint8_t* src_data = static_cast<const uint8_t*>(pixels);
 if (skip_size_in_bytes) { // <----
  src_data += skip_size_in_bytes;
 }

 if (!PackPixels(src_data, source_data_format,
                 unpack_params.row_length ? unpack_params.row_length : width,
                 height, gfx::Rect(0, 0, width, height), 1,
                 unpack_params.alignment, 0, format, type,
                 (premultiply_alpha ? kAlphaDoPremultiply : kAlphaDoNothing),
                 data.data(), flip_y))
  return false;

 return true;
}
```

Comment 1 by diehl...@microsoft.com on Wed, Mar 9, 2022, 7:14 PM EST Project Member

Description was changed.

Comment 2 by bookholt@chromium.org on Thu, Mar 10, 2022, 4:12 PM EST Project Member

Status: Assigned (was: Untriaged)
Owner: kainino@chromium.org
Cc: enga@chromium.org cwallez@chromium.org
Labels: FoundIn-99 Security_Severity-High OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2
Components: Blink>WebGL

Thanks for the report!

Practical reachability is difficult to verify, but assigning Severity High here on the basis of 3 observations:
1) Output from clang-analyzer indicates presence of a code path exists that can lead to memory corruption. In this case, an attacker may be able to influence the value of src_data [1] with an erroneous offset into the pixels buffer

attacker may be able to influence the value of src_data [1] with an erroneous offset into the pixels buffer.
2) Assume memory corruption can lead to RCE
3) This code runs in a sandboxed process

[1]
https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc;l=4003;drc=17bde68d075e4aa4c8b30dd1c587c54afdef58e2

Comment 3 by sheriffbot on Thu, Mar 10, 2022, 4:17 PM EST Project Member

Labels: Security_Impact-Stable

Comment 4 by sheriffbot on Fri, Mar 11, 2022, 12:48 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 5 by sheriffbot on Fri, Mar 11, 2022, 1:08 PM EST Project Member

Labels: -Pri-2 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 6 by cwallez@chromium.org on Tue, Mar 15, 2022, 2:54 PM EDT Project Member

GLenum WebGLImageConversion::ComputeImageSizeInBytes returns a GLenum for a GL error but it isn't checked. Maybe it should?

Comment 7 by adetaylor@google.com on Tue, Mar 22, 2022, 2:12 PM EDT Project Member

kainino@ seems to be OOO until 28th; pinged to ask them to take a look when they're back.

Comment 8 by sheriffbot on Thu, Mar 24, 2022, 12:21 PM EDT Project Member

kainino: 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 9 by kainino@chromium.org on Mon, Mar 28, 2022, 4:50 PM EDT Project Member

Owner: gman@chromium.org
Cc: kbr@chromium.org

My apologies, for some reason I didn't realize this was assigned to me. Let me try to find a better owner.

On inspection, I think cwallez@'s suspicion seems right.

Comment 10 by Git Watcher on Mon, Mar 28, 2022, 11:12 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f3244fe50ba6c64ab6a75f1370d8dd983927fae6

commit f3244fe50ba6c64ab6a75f1370d8dd983927fae6
Author: Gregg Tavares <gman@chromium.org>
Date: Tue Mar 29 03:11:52 2022

Check for error when calling ComputeImageSizeInBytes

~~Bug: chromium:1304987~~
Change-Id: I8311231156fca3200ce74d79db59d910a1a0e33a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556686
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Gregg Tavares <gman@chromium.org>
Cr-Commit-Position: refs/heads/main@{#986304}

[modify]
https://crrev.com/f3244fe50ba6c64ab6a75f1370d8dd983927fae6/third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc

Comment 11 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 12 by sheriffbot on Wed, Mar 30, 2022, 12:21 PM EDT Project Member

Labels: -M-99 M-100 Target-100

Comment 13 by sheriffbot on Thu, Apr 7, 2022, 12:21 PM EDT Project Member

gman: Uh oh! This issue still open and hasn't been updated in the last 28 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 sheriffbot on Mon, Apr 18, 2022, 11:10 AM EDT Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

Thanks for your time! To disable nags, add the Disable-Nags label.

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 15 by kbr@chromium.org on Mon, Apr 18, 2022, 3:53 PM EDT Project Member

Status: Fixed (was: Assigned)

Our understanding is that this has been fixed by https://chromium.googlesource.com/chromium/src/+/f3244fe50ba6c64ab6a75f1370d8dd983927fae6 .

Comment 16 by sheriffbot on Tue, Apr 19, 2022, 1:41 PM EDT Project Member

Labels: Restrict-View-SecurityNotify

Comment 17 by sheriffbot on Tue, Apr 19, 2022, 2:01 PM EDT Project Member

Labels: Merge-Request-101 Merge-Request-100 Merge-NA-102

Requesting merge to stable M100 because latest trunk commit (986304) appears to be after stable branch point (972766).

Requesting merge to beta M101 because latest trunk commit (986304) appears to be after beta branch point (982481).

Not requesting merge to dev (M102) because latest trunk commit (986304) appears to be prior to dev branch point (992738). If this is incorrect, please replace the Merge-NA-102 label with Merge-Request-102. If other changes are required to fix this bug completely, please request a merge if necessary.

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

Comment 18 by sheriffbot on Tue, Apr 19, 2022, 2:07 PM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 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: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 19 by sheriffbot on Tue, Apr 19, 2022, 2:07 PM EDT Project Member

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

Merge review required: M100 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:

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 20 by amyressler@chromium.org on Tue, Apr 19, 2022, 4:15 PM EDT Project Member

Labels: -Merge-Review-100 -Merge-Review-101 Merge-Approved-101 Merge-Approved-100

m101 and m100 merges approved; please merge ASAP to branches 4951 and 4896 respectively so this fix can be included in today's release cut of M101 stable and M100 extended. Sorry for the last minute ping, but since this issue was only updated as fixed earlier today, this didn't end up in security merge review queues until after final checks.

Please let me know if there are any issues or concerns with this. In the future, please update bug reports to Fixed once the resolving CLs have been landed. Thank you!

Comment 21 by Git Watcher on Tue, Apr 19, 2022, 7:42 PM EDT Project Member

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/96feac616a9d6adeef1da1c533b080bb3b9d53cc

commit 96feac616a9d6adeef1da1c533b080bb3b9d53cc
Author: Gregg Tavares <gman@chromium.org>
Date: Tue Apr 19 23:41:13 2022

Check for error when calling ComputeImageSizeInBytes

(cherry picked from commit f3244fe50ba6c64ab6a75f1370d8dd983927fae6)

~~Bug: chromium:1304987~~
Change-Id: I8311231156fca3200ce74d79db59d910a1a0e33a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556686
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Gregg Tavares <gman@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986304}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3593849
Auto-Submit: Gregg Tavares <gman@chromium.org>
Reviewed-by: Ben Mason <benmason@chromium.org>
Commit-Queue: Ben Mason <benmason@chromium.org>

Owners-Override: Ben Mason <benmason@chromium.org>
Commit-Queue: Kenneth Russell <kbr@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#902}

Cr-Commit-Position: refs/branch-heads/4951@{#902}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/96feac616a9d6adeef1da1c533b080bb3b9d53cc/third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc

Comment 22 by sheriffbot on Tue, Apr 19, 2022, 7:47 PM 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 23 by rzanoni@google.com on Wed, Apr 20, 2022, 12:22 PM EDT Project Member

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

Comment 24 by Git Watcher on Wed, Apr 20, 2022, 3:47 PM EDT Project Member

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d9b0bc0dcd437407a2403c54e0639a9943a4dab6

commit d9b0bc0dcd437407a2403c54e0639a9943a4dab6
Author: Gregg Tavares <gman@chromium.org>
Date: Wed Apr 20 19:46:07 2022

Check for error when calling ComputeImageSizeInBytes

(cherry picked from commit f3244fe50ba6c64ab6a75f1370d8dd983927fae6)

~~Bug: chromium:1304987~~
Change-Id: I8311231156fca3200ce74d79db59d910a1a0e33a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556686
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Gregg Tavares <gman@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986304}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3594708
Auto-Submit: Gregg Tavares <gman@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#1163}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/d9b0bc0dcd437407a2403c54e0639a9943a4dab6/third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc

_image_conversion.cc

Comment 25 by rzanoni@google.com on Mon, Apr 25, 2022, 3:16 PM EDT Project Member

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

Comment 26 by sheriffbot on Mon, Apr 25, 2022, 3:19 PM 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 27 by rzanoni@google.com on Mon, Apr 25, 2022, 3:22 PM EDT Project Member

1. Just https://crrev.com/c/3597078
2. Low, no conflicts
3. 100, 101
4. Yes

Comment 28 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:06 PM EDT Project Member

Labels: Release-0-M101

Comment 29 by gmpritchard@google.com on Tue, Apr 26, 2022, 10:35 AM EDT Project Member

Labels: LTS-Merge-Delayed-96

Comment 30 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT Project Member

Labels: CVE-2022-1482 CVE_description-missing

Comment 31 by gmpritchard@google.com on Thu, Apr 28, 2022, 10:32 AM EDT Project Member

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

Comment 32 by gmpritchard@google.com on Thu, Apr 28, 2022, 10:39 AM EDT Project Member

Labels: -LTS-Merge-Review-96

Comment 33 by Git Watcher on Fri, Apr 29, 2022, 11:24 AM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5be8e065f43e219d4ab71cefecdbbfd3e75ff426

commit 5be8e065f43e219d4ab71cefecdbbfd3e75ff426
Author: Gregg Tavares <gman@chromium.org>

Author: Gregg Tavares <gman@cnromium.org>
Date: Fri Apr 29 15:23:33 2022

[M96-LTS] Check for error when calling ComputeImageSizeInBytes

(cherry picked from commit f3244fe50ba6c64ab6a75f1370d8dd983927fae6)

~~Bug: chromium:1304987~~
Change-Id: I8311231156fca3200ce74d79db59d910a1a0e33a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556686
Commit-Queue: Gregg Tavares <gman@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986304}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3597078
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1609}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/5be8e065f43e219d4ab71cefecdbbfd3e75ff426/third_party/blink/renderer/platform/graphics/gpu/webgl_image_conversion.cc

Comment 34 by voit@google.com on Tue, May 17, 2022, 10:23 AM EDT Project Member

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

Comment 35 by sheriffbot on Tue, Jul 26, 2022, 1:29 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 36 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 37 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing