Starred by 3 users

Owner:	wtc@google.com
CC:	adetaylor@chromium.org gram...@twoorioles.com dalec...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Media
Modified:	Sep 8, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Merge-na
Security_Impact-Stable
Security_Severity-Medium
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
M-92
Target-92
external_security_report
LTS-Security-90
LTS-Security-Failed-90
Release-0-M92
CVE-2021-30578

Issue 1201074: Security: use-of-uninitialized-value in libavif when decode the crafted avif file

Reported by happy...@gmail.com on Wed, Apr 21, 2021, 2:08 AM EDT

Code

VULNERABILITY DETAILS
use-of-uninitialized-value in libavif when decode the crafted avif file

VERSION
latest libavif version

Since the chromium adopt the libavif as the codec to the avif format, this crash may also happened on the chrome when decode the avif file.

REPRODUCTION CASE
Build thee libavif library with memory sanitizer:

1. (Note that since the chromium reuse the source libavif of the github, I use the source of the github instead.)

2. git clone https://github.com/AOMediaCodec/av1-avif.git

3. build the dav1d with msan:

modify the ext/dav1d.cmd file in the root source, change the

meson --default-library=static --buildtype release ..

to

meson --default-library=static --buildtype release .. -Db_sanitize=memory

Then compile it running ./ext/dav1d.cmd

4. build the libavif avif_example_decode_file (example apps) with msan:

```
mkdir build
cd build
cmake -DBUILD_SHARED_LIBS=0 -DAVIF_CODEC_DAV1D=1 -DAVIF_LOCAL_DAV1D=1 -DAVIF_BUILD_EXAMPLES=1 ..
make avif_example_decode_file
```

5. run the avif_example_decode_file with the uploaded crash file:
./avif_example_decode_file avif-reformat-use-of-uninitialized-value.avif

Then the lib crash with the use-of-uninitialized.

Type of crash: Use-of-uninitialized-value
Crash State:

```
==115154==WARNING: MemorySanitizer: use-of-uninitialized-value
    #0 0x4c91b8 in avifImageYUVAnyToRGBAnySlow /libavif/src/reformat.c:584:84
    #1 0x4c91b8 in avifImageYUVToRGB /libavif/src/reformat.c:1212:29
    #2 0x494d37 in LLVMFuzzerTestOneInput /libavif/examples/decode_fuzzer.c:45:52
    #3 0x495acf in main /libavif/examples/decode_fuzzer.c:123:5
    #4 0x7faf61fa8bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310
    #5 0x41b8e9 in _start (/libavif/memory_build/decode_fuzzer+0x41b8e9)

SUMMARY: MemorySanitizer: use-of-uninitialized-value /libavif/src/reformat.c:584:84 in avifImageYUVAnyToRGBAnySlow
Exiting
```

CREDIT INFORMATION
Reporter credit: Chaoyuan Peng

[Deleted] **avif-reformat-use-of-uninitialized-value.avif**

Comment 1 by sheriffbot on Wed, Apr 21, 2021, 2:13 AM EDT

Labels: external_security_report

Comment 2 by carlosil@chromium.org on Thu, Apr 22, 2021, 7:55 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: wtc@google.com
Labels: Security_Impact-Stable Security_Severity-Medium
Components: Blink>Media

Triaging as medium severity since libavif is used in the renderer. wtc: Passing to you since you are listed as a libavif owner. Can you help further triage this one (and reassign as appropriate)? Thanks.

Comment 3 by carlosil@chromium.org on Thu, Apr 22, 2021, 7:55 PM EDT

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

Comment 4 by wtc@google.com on Thu, Apr 22, 2021, 8:00 PM EDT

Status: Started (was: Assigned)

happyercat: Thank you very much for the bug report. I will take a look.

Comment 5 by sheriffbot on Fri, Apr 23, 2021, 1:02 PM EDT

Labels: M-91 Target-91

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 6 by sheriffbot on Fri, Apr 23, 2021, 1:38 PM EDT

Labels: -Pri-3 Pri-1

Setting Pri-1 to match security severity Medium. 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 7 by wtc@google.com on Wed, Apr 28, 2021, 1:29 PM EDT

Cc: gram...@twoorioles.com

I tracked down the bug. The uninitialized memory error is in dav1d. I wrote a fix at https://code.videolan.org/videolan/dav1d/-/merge_requests/1194.

The bug occurs when the frame uses film grain synthesis (it may require certain film grain parameters, I did not look closely), has an odd number of rows, and chroma is subsampled vertically (i.e., YUV 4:2:0). Under these conditions, the last row of the chroma planes contains uninitialized values for column indexes >= half of the stride.

Notes:

1. The steps to reproduce the bug in the original description have some errors. Fortunately I can build dav1d and libavif with msan in Google's internal source repository.

2. I cannot reproduce the error using avif_example_decode_file, but I can reproduce it using avifenc and avif_decode_fuzzer. Note that the stack trace in the original description is a stack trace from avif_decode_fuzzer, not avif_example_decode_file.

Comment 8 by wtc@google.com on Wed, Apr 28, 2021, 1:33 PM EDT

Cc: dalec...@chromium.org

I believe this bug also affects AV1 videos, even though the reproducer test case is an AVIF image.

Comment 9 by wtc@google.com on Wed, Apr 28, 2021, 5:36 PM EDT

It turns out that this bug was independently discovered by Google's internal ClusterFuzz on Feb 27, 2021 (b/181396790). Regrettably I failed to track down that bug quickly, and then ClusterFuzz closed that bug later because some change to libavif made the reproducer testcase fail the avifDecoderParse() call in avif_decoder_fuzzer.cc.

Comment 10 Deleted

Comment 11 by wtc@google.com on Fri, Apr 30, 2021, 12:09 PM EDT

Hi happyercat,

My fix for dav1d has not been merged: https://code.videolan.org/videolan/dav1d/-/merge_requests/1194.

A poc of AV1 video would be helpful but is not necessary. (I believe we can create one by extracting the AV1 bitstream out of avif-reformat-use-of-uninitialized-value.avif and putting it in an IVF file.)

Comment 12 by carlosil@chromium.org on Fri, Apr 30, 2021, 2:46 PM EDT

Cc: adetaylor@chromium.org

Re #10: cc-ing adetaylor for the VRP and CVE questions, because I'm not sure about eligibility since the internal fuzzer had also discovered the bug.

Comment 13 by Git Watcher on Fri, Apr 30, 2021, 9:28 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7dca464eca4c9f062b8b6532b51ab92211634bf6

commit 7dca464eca4c9f062b8b6532b51ab92211634bf6
Author: Wan-Teh Chang <wtc@google.com>
Date: Sat May 01 01:27:07 2021

Roll src/third_party/dav1d/libdav1d/ f06148e7c..136585101 (20 commits)

https://chromium.googlesource.com/external/github.com/videolan/dav1d.git/+log/f06148e7c755..136585101bd5

$ git log f06148e7c..136585101 --date=short --no-merges --format='%ad %ae %s'
2021-04-28 wtc Subsample out->p.h correctly in dav1d_apply_grain
2021-03-22 martin arm64: filmgrain: Add NEON implementation of the generate_grain_y function
2021-03-26 martin checkasm: Implement printing of grain lut entries
2021-04-26 martin arm64: filmgrain: Add the missing HIGHBD_DECL_SUFFIX for the fguv functions
2021-04-27 martin Remove a variable that is set but not used
2021-03-16 martin checkasm: filmgrain: Add a padded check for fgy and fguv
2021-03-16 martin checkasm: Extend the padding checker to allow for some amount of overwrite
2021-02-19 martin checkasm: ipred: Use the padded pixel checking function
2021-02-19 martin checkasm: Add macros for allocating and checking padded pixel buffers
2021-04-22 martin x86: Fix writes past the intended area in AVX2 fguv
2021-04-14 jamrial dav1d: add event flags to the decoding process
2021-03-22 martin arm64: filmgrain: Share the prologue of the fgy function
2021-03-15 martin arm64: filmgrain: Add NEON implementation of the fguv function
2021-03-24 martin attributes: Add a CHECK_OFFSET macro for verifying struct offsets
2021-03-21 martin checkasm: filmgrain: Check all overlap combinations in each run
2021-03-20 martin filmgrain: Use the BITDEPTH_MAX macro and round2 helper function
2021-04-02 code CI: Fix asm checks
2021-03-16 martin checkasm: Drop one layer of macro expansion for concatenation
2021-03-12 martin arm64: Add NEON implementation of fgy_32x32xn
2021-03-07 code CI: Add check for illegal instructions

Created with:
  roll-dep src/third_party/dav1d/libdav1d
R=dalecurtis@chromium.org

~~Bug: 1201074~~
Change-Id: I67be894a4c4a9ef41fa653fd6a3b27f252299531
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2863934
Reviewed-by: Dale Curtis <dalecurtis@chromium.org>
Commit-Queue: Wan-Teh Chang <wtc@google.com>
Cr-Commit-Position: refs/heads/master@{#878146}

[modify] https://crrev.com/7dca464eca4c9f062b8b6532b51ab92211634bf6/DEPS
[modify] https://crrev.com/7dca464eca4c9f062b8b6532b51ab92211634bf6/third_party/dav1d/dav1d_generated.gni

Comment 14 by wtc@google.com on Wed, May 5, 2021, 2:23 PM EDT

Hi Adrian (adetaylor),

This bug was assigned the target milestone M-91 by sheriffbot in comment 5. I think it is sufficient to fix this bug in M-92. May I change the milestone and target to M-92 and Target-92?

This bug affects AV1 videos and AVIF images only under the following conditions:

The bug occurs when the frame uses film grain synthesis (it may require certain film grain parameters, I did not look closely), has an odd frame height, and chroma is subsampled vertically (i.e., YUV 4:2:0). Under these conditions, the last row of the chroma planes contains uninitialized values for column indexes >= half of the stride.

Since frame height is usually an even number and film grain synthesis is not a commonly used feature, this combination is rare in practice.

Thank you.

Comment 15 by adetaylor@chromium.org on Wed, May 5, 2021, 6:10 PM EDT

Hi wtc, thanks for the thorough explanation!

First, could you mark this bug as Fixed if it's fixed? https://chromium.googlesource.com/chromium/src/+/master/docs/security/security-labels.md#TOC-Merge-labels - then Sheriffbot can add appropriate merge labels, this can go to the VRP panel, etc.

> Since frame height is usually an even number and film grain synthesis is not a commonly used feature, this combination is rare in practice.

I don't think that's relevant: An attacker can presumably craft such a file using whatever features they require to exploit this bug. Or, does Chrome reject such types of file before attempting to decode them?

This is medium severity, so we'd be pretty keen to merge this back to M91. Is your concern about the stability risk from a big roll of dav1d?

Comment 16 by wtc@google.com on Wed, May 5, 2021, 6:20 PM EDT

Status: Fixed (was: Started)

Hi Adrian,

Thank you for your reply. Yes, I am worried about the stability risk from a big roll of dav1d.

Comment 17 by sheriffbot on Thu, May 6, 2021, 12:43 PM EDT

Labels: reward-topanel

Comment 18 by adetaylor@google.com on Thu, May 6, 2021, 12:55 PM EDT

Labels: Merge-NA

OK. Let's keep this for M92 then. Thanks.

Comment 19 by wtc@google.com on Thu, May 6, 2021, 1:47 PM EDT

Labels: -M-91 -Target-91 M-92 Target-92

Comment 20 by sheriffbot on Thu, May 6, 2021, 2:02 PM EDT

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

Comment 21 by amyressler@google.com on Thu, May 20, 2021, 1:08 PM EDT

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 22 Deleted

Comment 23 by amyressler@chromium.org on Thu, May 20, 2021, 5:28 PM EDT

Congratulations, Chaoyuan Peng! The VRP Panel has decided to award you $7500 for this report. A member of our finance team will be in touch in the coming days to arrange payment. Nice work!

Comment 24 by amyressler@google.com on Fri, May 21, 2021, 5:30 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@chromium.org on Mon, Jul 19, 2021, 4:16 PM EDT

Labels: Release-0-M92

Comment 26 by amyressler@google.com on Mon, Jul 19, 2021, 7:17 PM EDT

Labels: CVE-2021-30578 CVE_description-missing

Comment 27 by amyressler@google.com on Tue, Aug 3, 2021, 3:42 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 28 by sheriffbot on Thu, Aug 12, 2021, 1:29 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 29 by janag...@google.com on Wed, Sep 8, 2021, 11:36 AM EDT

Labels: LTS-Security-90 LTS-Security-Failed-90

Skipping for LTS due to comment 16.