☆ Starred by 2 users

Owner:	jonat...@arm.com
CC:	scro...@google.com cblume@chromium.org
Status:	Verified *(Closed)*
Components:	Internals>Images>Codecs
Modified:	Nov 16, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Lacros
Pri:	2
Type:	Bug-Security

reward-5000
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-91
Release-0-M94
CVE-2021-37972

Issue 1234259: Security: a READ memory access in jsimd_huff_encode_one_block_sse2

Reported by mundi...@gmail.com on Thu, Jul 29, 2021, 1:55 AM EDT

Code

# VULNERABILITY DETAILS

a READ memory access in jsimd_huff_encode_one_block_sse2

# VERSION

commit: 84d6306f64afd189de148ff13895537a24a55dd3
git repo:https://github.com/libjpeg-turbo/libjpeg-turbo

# REPRODUCTION CASE

./jpegtran(-static) -outfile x @@

There are four different situations at runtime:

## jpegtran with ASAN

./jpegtran -outfile x ./testcase

```
Corrupt JPEG data: 1 extraneous bytes before marker 0xda
AddressSanitizer:DEADLYSIGNAL
=================================================================
==96684==ERROR: AddressSanitizer: SEGV on unknown address 0x7fb6e2dc70a0 (pc 0x7fb6e2d6fdf4 bp 0x00000000fe80 sp 0x7ffef62ea720 T0)
==96684==The signal is caused by a READ memory access.
    #0 0x7fb6e2d6fdf4 in jsimd_huff_encode_one_block_sse2 (/home/kali/libjpeg-turbo/memtest/libjpeg.so.62+0x142df4)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/kali/libjpeg-turbo/memtest/libjpeg.so.62+0x142df4) in jsimd_huff_encode_one_block_sse2
==96684==ABORTING
```

## jpegtran without compiler and linker flags

./jpegtran -outfile x ./testcase

normal operation

## jpegtran-static with ASAN

./jpegtran-static -outfile x ./testcase

normal operation

## jpegtran-static without compiler and linker flags

./jpegtran-static -outfile x ./testcase

```
Corrupt JPEG data: 1 extraneous bytes before marker 0xda
zsh: segmentation fault  ../debug/jpegtran-static -outfile mmm ../memtest/plot/crash/0005
```

segmentation fault at jsimd_huff_encode_one_block_sse2()

CREDIT INFORMATION

Xu Hanyu and Lu Yutao from Panguite-Forensics-Lab of Qianxin

0005
324 bytes View Download

Comment 1 by sheriffbot on Thu, Jul 29, 2021, 1:59 AM EDT Project Member

Labels: external_security_report

Comment 2 by mea...@chromium.org on Thu, Jul 29, 2021, 8:58 AM EDT Project Member

jonathan.wright, could you please take a look at this one as well? Is this also in unreachable code as in ~~bug 1231868~~?

Comment 3 by mea...@chromium.org on Thu, Jul 29, 2021, 8:58 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: jonat...@arm.com

(Actually assigning the bug)

Comment 4 by mea...@chromium.org on Fri, Jul 30, 2021, 7:52 AM EDT Project Member

Labels: Security_Severity-Low FoundIn-91 OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros
Components: Internals>Images>Codecs

Tentatively adding labels. Low severity as this is a single byte read.

Comment 5 by sheriffbot on Fri, Jul 30, 2021, 7:54 AM EDT Project Member

Labels: Security_Impact-Stable

Comment 6 by sheriffbot on Fri, Jul 30, 2021, 1:24 PM EDT Project Member

Labels: -Pri-3 Pri-2

Setting Pri-2 to match security severity Low. 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 jonat...@arm.com on Tue, Aug 3, 2021, 9:10 AM EDT Project Member

Status: Started (was: Assigned)
Cc: cblume@chromium.org scro...@google.com

This bug seems a bit more worrying as there's a crash inside the libjpeg.so - which shouldn't happen, regardless of the data fed into it.

On further investigation, the bug causing the crash is only present on x86_64 platforms - I could not reproduce the crash on AArch64 Linux or Apple Silicon MacOS when building libjpeg-turbo in either Debug or Release modes.

Digging further into the x86_64 Linux builds, things get interesting:

For Release builds, "./jpegtran -outfile x ./testcase" and "./jpegtran-static -outfile x ./testcase" both result in a segfault.

For Debug builds, however, "./jpegtran -outfile x ./testcase" does not result in a crash, while "./jpegtran-static -outfile x ./testcase" does.

Running under GDB to figure out what's happening:

For Release builds, "./jpegtran -outfile x ./testcase" results in a segfault but "./jpegtran-static -outfile x ./testcase" does *not*.

For Debug builds, *neither* "./jpegtran -outfile x ./testcase" nor "./jpegtran-static -outfile x ./testcase" result in a crash.

The most information I can get out of GDB for a Release build is:

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7f7b694 in jsimd_huff_encode_one_block_sse2 ()
   from /chromium/x86-build-libjpeg-turbo/x86-build/libjpeg.so.62
(gdb) bt
#0  0x00007ffff7f7b694 in jsimd_huff_encode_one_block_sse2 ()
   from /chromium/x86-build-libjpeg-turbo/x86-build/libjpeg.so.62
#1  0x000055555557ba00 in ?? ()
#2  0x0000000000000000 in ?? ()
```

It seems we have a classic Heisenbug on our hands... I'll report it to the upstream project maintainer to see if he can offer any assistance.

Comment 8 by jonat...@arm.com on Tue, Aug 3, 2021, 9:46 AM EDT Project Member

Reported to the upstream project.[1]

[1] https://github.com/libjpeg-turbo/libjpeg-turbo/issues/543

Comment 9 by sheriffbot on Thu, Aug 5, 2021, 1:41 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 10 by sheriffbot on Fri, Aug 6, 2021, 12:21 PM EDT Project Member

Labels: -Security_Impact-Extended

Comment 11 by sheriffbot on Fri, Aug 6, 2021, 12:27 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 12 by sheriffbot on Fri, Aug 6, 2021, 1:28 PM EDT Project Member
Labels: -Security_Impact-Extended Security_Impact-Stable

Comment 13 by Git Watcher on Tue, Aug 10, 2021, 10:16 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/deps/libjpeg_turbo/+/ff19e5b2e176c61d552f68768e0e051867745321

commit ff19e5b2e176c61d552f68768e0e051867745321
Author: Jonathan Wright <jonathan.wright@arm.com>
Date: Mon Aug 09 09:09:36 2021

Update libjpeg-turbo to 2.1.1 stable release

Notable changes include a fix for a crash in the 64-bit SSE2 Huffman
encoder.

~~Bug: 1234259~~
Change-Id: Id764c5d8485f095a693504580d9ad81ba860d3ae

[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/ChangeLog.md
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/README.chromium
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jconfig.h
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jconfigint.h
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jcphuff.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jdhuff.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jmemmgr.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jpegint.h
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jpegtran.1
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/jpegtran.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/simd/x86_64/jchuff-sse2.asm
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/transupp.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/transupp.h
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/turbojpeg.c
[modify] https://crrev.com/ff19e5b2e176c61d552f68768e0e051867745321/usage.txt

Comment 14 by Git Watcher on Tue, Aug 10, 2021, 1:26 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/98907227c199b72fcfa1e179f0c1d528fa17e093

commit 98907227c199b72fcfa1e179f0c1d528fa17e093
Author: Jonathan Wright <jonathan.wright@arm.com>
Date: Tue Aug 10 17:25:06 2021

Roll src/third_party/libjpeg_turbo/ ad8b3b0f8..ff19e5b2e (1 commit)

https://chromium.googlesource.com/chromium/deps/libjpeg_turbo.git/+log/ad8b3b0f84ba..ff19e5b2e176

```
$ git log ad8b3b0f8..ff19e5b2e --date=short --no-merges --format='%ad %ae %s'
2021-08-09 jonathan.wright Update libjpeg-turbo to 2.1.1 stable release
```

Created with:
roll-dep src/third_party/libjpeg_turbo

~~Bug: 1234259~~
Change-Id: I352f4b4fec2433e958c4ff076ee9441f2bcc0105
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3085668
Commit-Queue: Leon Scroggins <scroggo@google.com>
Auto-Submit: Jonathan Wright <jonathan.wright@arm.com>
Reviewed-by: Leon Scroggins <scroggo@google.com>
Cr-Commit-Position: refs/heads/master@{#910376}

[modify] https://crrev.com/98907227c199b72fcfa1e179f0c1d528fa17e093/DEPS

Comment 15 by jonat...@arm.com on Tue, Aug 10, 2021, 1:53 PM EDT Project Member
Status: Verified (was: Started)

Comment 16 by sheriffbot on Wed, Aug 11, 2021, 12:41 PM EDT Project Member
Labels: reward-topanel

Comment 17 by sheriffbot on Wed, Aug 11, 2021, 1:41 PM EDT Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 18 by amyressler@chromium.org on Mon, Sep 20, 2021, 6:06 PM EDT Project Member
Labels: Release-0-M94

Comment 19 by amyressler@google.com on Tue, Sep 21, 2021, 1:19 PM EDT Project Member
Labels: CVE-2021-37972 CVE_description-missing

Comment 20 by amyressler@google.com on Tue, Sep 28, 2021, 4:21 PM EDT Project Member
Labels: -reward-topanel reward-unpaid reward-5000

*** 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 21 by amyressler@chromium.org on Tue, Sep 28, 2021, 6:11 PM EDT Project Member

Congratulations, Xu Hanyu and Lu Yutao! The VRP Panel has decided to award you $5,000 for this report. A member of our finance team will be in touch in the coming days to arrange payment. Thank you for this report and nice work!

Comment 22 by amyressler@google.com on Fri, Oct 1, 2021, 11:42 AM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 23 by amyressler@google.com on Fri, Oct 8, 2021, 5:31 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 24 by sheriffbot on Tue, Nov 16, 2021, 1:32 PM EST 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