Merged 757660 tiff: cap buffer growth to prevent OOM from malicious IFD offset

Change Info

Show All

Sign in

Submitted	Mar 23
Owner	GerritBot
Uploader	Gopher Robot
Author	Andy | ZephrFish
Reviewers	Ian Lance Tayl... +2 Carlos Amedee +1 Dmitri Shuraly... +1 Dmitri Shuraly... Gopher Robot Go LUCI
CC	Nigel Tao Andy Gill
Repo | Branch	image | master
Hashtags	no-owners

```
tiff: cap buffer growth to prevent OOM from mal

A crafted 8-byte TIFF file with IFD offset 0xFF
buffer.fill() to allocate ~4GB of memory when d
io.Reader (non-ReaderAt path), leading to an ou
crash in any Go application that calls Decode o
on untrusted input.

Read the data, and allocate the buffer, in chun
to limit memory allocation to the size of the i

References: https://issuetracker.google.com/iss
Fixes golang/go#78267

Change-Id: I514161af87fb3ad24180ec4bed61fa49f49
GitHub-Last-Rev: 8e6d97892cfbdea81fa9e9ec3e3872
```

Show All

Submit Requirements

Code-Review	+2 +1
No-Unresolved-Comments	Satisfied
Review-Enforcement	Satisfied
TryBots-Pass	+1

Comments 13 resolved

Checks Loading results

Trigger Votes

Auto-Submit +1

Files Comments Checks

Base → Patchset 7 23ae9ed Download Expand All

File	C	Delta
Commit message		
M .../buffer.go		-17 +16
M .../reader_test.go		-0 +31
		-17 +47

Change Log

Show all entries (13 hidden) Expand All

Gopher Robot	1	I spotted some possible problems with your PR: 1. You ...	Patchset 1 | Mar 20 11:29 PM
Gopher Robot		Congratulations on opening your first change. Thank you for y...	Patchset 1 | Mar 20 11:32 PM
Gopher Robot		Hashtag added: no-owners	Patchset 1 | Mar 20 11:40 PM
Andy Gill	1	Done	Patchset 1 | Mar 21 4:22 AM
Ian Lance Taylor	1		Patchset 2 | Mar 21 8:24 AM
Andy Gill	1	Thanks Ian, good suggestion. I've updated the CL to foll...	Patchset 2 | Mar 21 11:17 AM
Ian Lance Taylor	2		Patchset 3 | Mar 22 8:57 AM
Ian Lance Taylor		Commit-Queue +1	Patchset 4 | Mar 22 9:22 PM
Go LUCI		This CL has passed the run	Patchset 4 | Mar 22 9:26 PM
Andy Gill	1		Patchset 4 | Mar 22 10:19 PM
Andy Gill	1		Patchset 4 | Mar 23 12:06 AM
Ian Lance Taylor	2		Patchset 4 | Mar 23 4:51 AM
Andy Gill	3	Fixed both and pushed to branch	Patchset 4 | Mar 23 10:44 AM
GerritBot		Uploaded patch set 5. Outdated Votes: * LUCI-Tr... View Diff	Patchset 5 | Mar 23 10:46 AM
Ian Lance Taylor	1		Patchset 5 | Mar 23 11:00 AM
Andy Gill	1	Done. Squashed into one commit with a tidied descripti...	Patchset 5 | Mar 23 11:19 AM
Andy Gill	2	Done	Patchset 5 | Mar 23 11:19 AM
GerritBot		Uploaded patch set 6: Commit message was up... View Diff	Patchset 6 | Mar 23 11:34 AM
Ian Lance Taylor		Code-Review +2 Commit-Queue +1	1 Thanks. Patchset 6 | Mar 23 11:42 AM
Go LUCI		Dry run: CV is trying the patch. Bot data: {"action":"start","trigg...	Patchset 6 | Mar 23 11:42 AM
Go LUCI on behalf of Ian Lance Taylor		Commit-Queue 0 (vote reset) (Perform...	Patchset 6 | Mar 23 11:47 AM
Go LUCI		This CL has passed the run	Patchset 6 | Mar 23 11:47 AM
Go LUCI		LUCI-TryBot-Result +1	Patchset 6 | Mar 23 11:47 AM
Dmitri Shuralyov		Added to cc: Nigel Tao Dmitri Shuralyov Added to revie\	Patchset 6 | Mar 23 2:42 PM
Dmitri Shuralyov		Code-Review +1	Patchset 6 | Mar 23 2:42 PM
Carlos Amedee		Added to reviewer: Carlos Amedee	Patchset 6 | Mar 23 3:30 PM
Carlos Amedee		Code-Review +1	Patchset 6 | Mar 23 3:30 PM

Andy Gill	1 Is there anything else required from my side for this to b…	Patchset 6 | Mar 23 7:40 PM
Dmitri Shuralyov	Moved from cc to reviewer: Dmitri Shuralyov	Patchset 6 | Mar 23 7:55 PM
Dmitri Shuralyov	Auto-Submit +1 2 Thanks.	Patchset 6 | Mar 23 7:55 PM
Gopher Robot	Moved from cc to reviewer: Gopher Robot	Patchset 6 | Mar 23 7:58 PM
Gopher Robot	Change has been successfully cherry-picked as 23ae9ed61c1d…	Patchset 7 | Mar 23 7:58 PM