Gmail **ChiJin Zhou <tlock.chijin@gmail.com>**

A potential vulnerability

3 messages

ChiJin Zhou <tlock.chijin@gmail.com> Sun, Jun 3, 2018 at 5:13 PM
To: jpeg-info@jpegclub.org

Hi

I recently find a strange phenomenon that cjpeg sometimes compresses a small input file into a large output file in version 9c.
For example, when https://github.com/ChijinZ/security_advisories/blob/master/others/large_loop is input into cjpeg (command: .lib/cjpeg large_loop > out),
It takes a long time (~6 min) to finish the compression and output a 21979501 bytes output file while the input file is 6142 bytes.
I think it is a potential vulnerability and look forward your fixing.

Chijin Zhou

Guido Vollbeding <guido@jpegclub.org> Mon, Jun 4, 2018 at 1:08 AM
To: ChiJin Zhou <tlock.chijin@gmail.com>

Hi ChiJin Zhou

Thank you for feedback.

Will fix in next release:

rdtarga.c: use read_byte(), with EOF check, instead of getc() in read_pixel().
Thank to Chijin Zhou for cjpeg potential vulnerability report.

The next version (9d) is planned for release in January 2020.
A pre-release package will be provided in 2019 on http://jpegclub.org/reference/reference-sources/, I will send you a notification.

Kind regards
Guido Vollbeding
Organizer Independent JPEG Group

ChiJin Zhou <tlock.chijin@gmail.com> Mon, Jun 4, 2018 at 1:17 AM
To: Guido Vollbeding <guido@jpegclub.org>

Thank you for the update.

Guido Vollbeding <guido@jpegclub.org>于2018年6月4日 周一上午1:08写道：
[Quoted text hidden]