

Forum:[Hack Forums](#)

Thread: [To the people who think jpeg exploits are "BS"](#)

?Criminal - October 11, 2016, 5:20 pm

<https://fossbytes.com/warning-just-opening-jpeg-2000-image-file-can-get-hacked/>

this seems to only effect the jpeg2000 format which is slightly different then normal .jpeg files but opening pdfs with these embedded images is enough to get owned. Alot of people tend to think .jpeg exploits are far fetched but as you can see here they do come through the pipeline occasionally your just not gonna find exploits that target windows photo viewer or similar things.

Faith Connors - October 11, 2016, 5:37 pm

Good shit, this is a really neat find.

But just out of curiosity, if anyone knows more about memory than me, how far could you potentially go with this? As we can see there is a segfault at the end of the full documentation on the Talos site, which means that the application crashes. So how would you be able to stop that crash and actually execute some kind of code?

Also there is an exploit kit available for images, but it works very differently as it's for hiding code in an image file which is virtually undetectable. Have a look at Stegosplit.

Mr. Robot - October 11, 2016, 5:44 pm

Been trying to find a post regarding it in detail for a while.

Faith Connors - October 11, 2016, 5:46 pm

(Oct 11, 2016 05:44 PM)Mr. Robot Wrote: [\[CITE\]](#) Been trying to find a post regarding it in detail for a while.

-snip-

The official documentation for it is pretty detailed

<http://www.talosintelligence.com/reports/TALOS-2016-0193/>

LanMan - October 11, 2016, 10:33 pm

(Oct 11, 2016 05:20 PM)?Criminal Wrote: [\[CITE\]](#) this seems to only effect the jpeg2000 format which is slightly different then normal .jpeg files but opening pdfs with these embedded images is enough to get owned.

Alot of people tend to think .jpeg exploits are far fetched but as you can see here they do come through the pipeline occasionally your just not gonna find exploits that target windows photo viewer or similar things.

The exploit is just for the codec parsing the jpeg2000 (OpenJPEG), not all app using this format will be vulnerable.

And one of the most used way to crack and flash the PSP was by using a image, a exploit in the libTIFF library

(Oct 11, 2016 05:37 PM)Faith Connors Wrote: [\[CITE\]](#) How far could you potentially go with this? As we can see there is a segfault at the end of the full documentation on the Talos site, which means that the application crashes. So how would you be able to stop that crash and actually execute some kind of code? By using multiple time the exploit they arrive to the point of Code Execution by

memory corruption.

In theory you could relocate and make a huge trampoline to continue the flow of the program, but since the exploit is based on wrong headers of the file and memory corruption it will still crash

somejohndue - October 12, 2016, 3:09 am

(Oct 11, 2016 10:33 PM)LanMan Wrote: [\[CITE\]](#) The exploit is just for the codec parsing the jpeg2000 (OpenJPEG), not all app using this format will be vulnerable.

And one of the most used way to crack and flash the PSP was by using a image, a exploit in the libTIFF library

By using multiple time the exploit they arrive to the point of Code Execution by memory corruption.

In theory you could relocate and make a huge trampoline to continue the flow of the program, but since the exploit is based on wrong headers of the file and memory corruption it will still crashA trampoline? I'd prefer a slide ;)

LanMan - October 12, 2016, 9:06 am

(Oct 12, 2016 03:09 AM)somejohndue Wrote: [\[CITE\]](#) A trampoline? I'd prefer a slide ;)

I'm not sure it will work as well, maybe try a swing ?

somejohndue - October 12, 2016, 9:20 am

(Oct 12, 2016 09:06 AM)LanMan Wrote: [\[CITE\]](#) I'm not sure it will work as well, maybe try a swing ? Referred to a NOP sled as the slide. Also there's a common association between the Global Offset Table and a trampoline (it launches off your vtable, function pointers etc), so not so far fetched.

LanMan - October 12, 2016, 2:53 pm

(Oct 12, 2016 09:20 AM)somejohndue Wrote: [\[CITE\]](#) Referred to a NOP sled as the slide.

Oh my bad, i though it was just a random joke ?

officeunit247 - August 6, 2019, 1:43 am

(Oct 11, 2016 05:20 PM)?Criminal Wrote: [\[CITE\]](#) this seems to only effect the jpeg2000 format which is slightly different then normal .jpeg files but opening pdfs with these embedded images is enough to get owned.Alot of people tend to think .jpeg exploits are far fetched but as you can see here they do come through the pipeline occasionally your just not gonna find exploits that target windows photo viewer or similar things.

i have bought the silent jpeg exploit form Odayexploits.org its working one pop up but its working exploit i paid 750\$ for this exploit but i am happy its working exploit

SlowMehMo - August 9, 2019, 2:11 am

(Aug 6, 2019 01:43 AM)officeunit247 Wrote: [\[CITE\]](#) i have bought the silent jpeg exploit form Odayexploits.org its working one pop up but its working exploit i paid 750\$ for this exploit but i am happy its working exploit

you paid 750 smackaroos for a exploit that will be patched soon and has a pop up requiring user action?

oh dear, sorry but yeah, you got scamzored.

greghoglund1204 - December 17, 2019, 10:32 pm

I have also found an exploit in jpeg2000. But are there any exploits in the native jpeg file? As far as I know, there was a big "windows XP photo viewer" exploit in 2004. But not found anything in windows 7 or later OS versions. Can anyone say about this?

