

Forum:[Hack Forums](#)

Thread: [Hack through instagram messages ?](#)

Alnut - April 27, 2024, 5:26 pm

Does anybody know if there are ways to say send an image via instagram DM to hack somebody

So like hide a payload in the image ? then send it as a disappearing message ?

Alnut - April 27, 2024, 5:34 pm

(Apr 27, 2024 05:29 PM)Lowicon Wrote: [\[CITE\]](#) Go ahead and ping me in a message I can help you.

I can't do that, as i need 25 posts apparently. I don't think you can respond either without having 25 posts. :-(

Absence - April 27, 2024, 5:54 pm

Anytime you upload an image to a social media platform, like instagram, the file is automatically modified so that it is easier for their services.

"They resize it, recompress it, strip metadata off it (largely for privacy and space saving reasons - there's no need to store random metadata, and geolocation tagged photos can leak your exact location), and may even crop or colour-correct the image. It makes sharing these kinds of files on those platforms very difficult."

Some further reading here, and also more technical explanation for your answers:

<https://security.stackexchange.com/questions/237715/if-malware-can-be-attached-to-an-image-file-then-why-arent-images-a-common-att>

Basically: if it was that easy, there would be a lot of people doing it. And if it is ever that easy, they'll do it, and they'll fix it.

Hope this helps!

Also, be wary of messaging random people off the site. Do not exchange money with some random person on here, who says they can do this. Utilize a middleman, a contract, and trade safely. Check out the [Help Docs](#)

DramaKing - April 27, 2024, 7:14 pm

(Apr 27, 2024 05:26 PM)Alnut Wrote: [\[CITE\]](#) Does anybody know if there are ways to say send an image via instagram DM to hack somebody

So like hide a payload in the image ? then send it as a disappearing message ?

Ignore the scammer. Whatever it is that he's offering, it won't be what you're asking for. What you're asking for is the WebP exploit found in Instagram documented as CVE-2023-4863. You can check it out below for historical purposes.

https://www.darknavy.org/blog/exploiting_the_libwebp_vulnerability_part_1/

Put another way you can certainly hide a payload in an image, but even if it doesn't break when processed, getting the code to execute would be monumental.

Alnut - April 27, 2024, 8:54 pm

(Apr 27, 2024 05:54 PM)Absence Wrote: [\[CITE\]](#) Anytime you upload an image to a social media platform, like instagram, the file is automatically modified so that it is easier for their services.

"They resize it, recompress it, strip metadata off it (largely for privacy and space saving reasons - there's no need to store random metadata, and geolocation tagged photos can leak your exact location), and may even crop or colour-correct the image. It makes sharing these kinds of files on those platforms very difficult."

Some further reading here, and also more technical explanation for your answers:

Basically: if it was that easy, there would be a lot of people doing it. And if it is ever that easy, they'll do it, and they'll fix it.

Hope this helps!

Also, be wary of messaging random people off the site. Do not exchange money with some random person on here, who says they can do this. Utilize a middleman, a contract, and trade safely. Check out the

Thank you very much for getting in touch and I appreciate the advise. However, are you able to confirm what Dramaking has stated that there does appear to be a loop hole of some sorts utilising webp ?

(Apr 27, 2024 07:14 PM)DramaKing Wrote: [\[CITE\]](#) Ignore the scammer. Whatever it is that he's offering, it won't be what you're asking for. What you're asking for is the WebP exploit found in Instagram documented as CVE-2023-4863. You can check it out below for historical purposes.

Put another way you can certainly hide a payload in an image, but even if it doesn't break when processed, getting the code to execute would be monumental.

Can you confirm if this was patched or still a "vulnerability"

So in short even if you could send the payload, it would be super difficult to execute ? Right.

Thanks again for posting the link, it was an interesting read and you certainly know your stuff :-)

DramaKing - April 28, 2024, 5:11 am

So here's the more detailed explanation. What you need is a zero-day, meaning that the developer doesn't know about it. This one was the 4863 vulnerability in 2023, so it's like a 216-day. Victim would need like Chrome 116.

I found the one that I was actually thinking of that affected the app. It was found back in 2020. Dang companies fixing these bugs.

<https://www.zdnet.com/article/instagram-bug-opened-a-path-for-hackers-to-hijack-app-turn-smartpho>

