Check Point reveals vulnerability found in Instagram

Instagram is one of the most popular social media platforms globally, with over 100+ million photos uploaded every day, and nearly 1 billion monthly active users. Individuals and companies share photos and messages about their lives and products to their followers globally.

So imagine what could happen if a hacker was able to completely take over Instagram accounts, and access all the messages and photos in those accounts, post new photos or delete or manipulate existing photos. What could that do to a person's or company's reputation?

Photo by energepic.com© from Pexels

Earlier this year, Check Point researchers found a critical vulnerability in the Instagram app that would have given an attacker the ability to take over a victim's Instagram account, and turn their phone into a spying tool, simply by sending them a malicious image file. When the image is saved and opened in the Instagram app, the exploit would give the hacker full access to the victim's Instagram messages and images, allowing them to post or delete images at will, as well as giving access to the phone's contacts, camera and location data.

Here's how researchers found the vulnerability and worked with Facebook and Instagram to close it to keep users safe.

What are the apps on your phone permitted to do?

Wherever we go, our mobile phones usually go with us, to keep us in touch with families, loved ones and our work, too. Of course, this is also why mobiles are an attractive target for hackers.

Not only can they steal data and credentials from our phones, but they can also use them for spying on us: tracking our location, listening to conversations, and accessing our data and messages.

Fortunately, all modern mobile operating systems include several layers of protection against this type of malicious activity. These protections usually rely on the basic concept of 'application isolation' – even if someone was able to hack a specific application, they would still be confined to that application alone, along with its strict permissions, and would not be able to extend their hacking attempt any further.

The key term here is "strict permissions" – for example, a map application should be able to access your location, but should not have access to your microphone; a dating app should be able to access your camera and nothing else, and so on.

But what happens when we're talking about an application that has extensive permissions on your device? If the application is hacked, the hacker will have easy access to your GPS data, camera, microphone, contacts, and more.

Fortunately, there isn't a huge list of apps that have such extensive permissions on users' devices. One example is Instagram. Given its popularity and wide-ranging permissions, we decided to review the security of Instagram's mobile app for both Android and iOS operating systems.

What was found?

The research revealed a critical vulnerability that might allow the attackers what is technically referred to as - remote code execution (RCE). This vulnerability can allow an attacker to perform any action they wish in the Instagram app (yes, even if it is not actually a part of the application logic or features). Since the Instagram app has very extensive permissions, this may allow an attacker to instantly turn the targeted phone into a perfect spying tool - putting the privacy of millions of users at serious risk.

Modus operandi

So how does such a popular application include vulnerabilities, when huge amounts of time and resources are invested in developing it?

The answer is that most modern app developers do not actually write the entire application on their own: if they did so it would take years to write an application. Instead, they use third party libraries to handle common (and often complicated) tasks such as image processing, sound processing, network connectivity, and so on. This frees the developers to handle only the coding tasks, which represent the apps core business logic. However, this relies on those 3rd party libraries being completely trustworthy and secure.

The modus operandi for this research was to examine the third party libraries used by Instagram.

The vulnerability found was in the way that Instagram used Mozjpeg - an open source project used by Instagram as its JPEG format image decoder for images uploaded to the service.

A bad image: hacking and taking over the user's mobile Instagram account

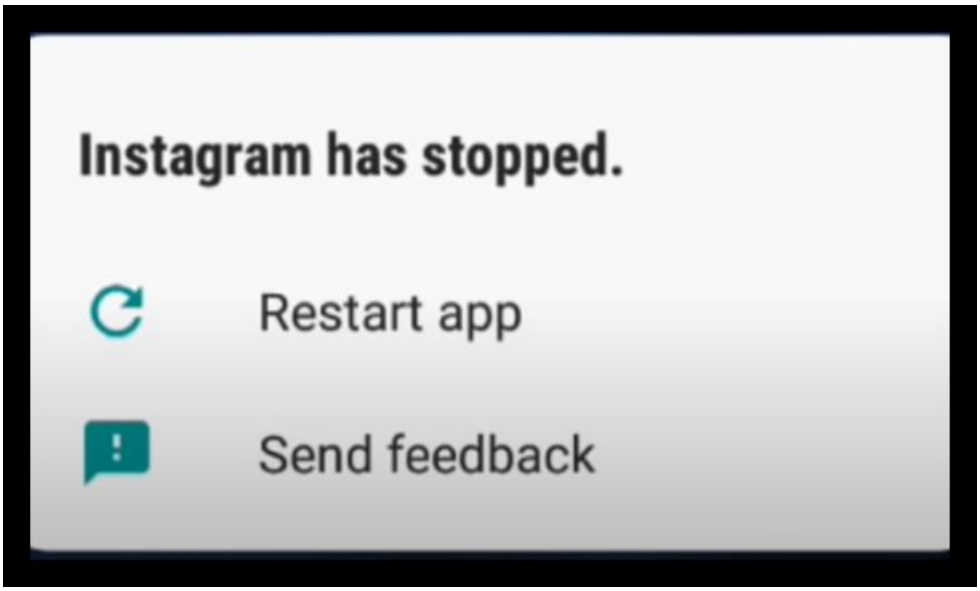
In the attack scenario describe in the research, an attacker can simply send an image to their target victim via email, WhatsApp or another media exchange platform. The target user saves the image on their handset, and when they open the

Instagram app, the exploitation takes place, allowing the attacker full access to any resource in the phone that is pre-allowed by Instagram.

These resources include contacts, device storage, location services and the device camera. In effect, the attacker gets full control over the app and can create actions on behalf of the user, including reading all of their personal messages in their Instagram account and deleting or posting photos at will.

This turns the device into a tool for spying on targeted users without their knowledge, as well as enabling malicious manipulation of their Instagram profile. In either case, the attack could lead to a massive invasion of users' privacy and could affect reputations – or lead to security risks that are even more serious.

At a basic level, this exploit can be used to crash a user's Instagram app, effectively denying them access to the app until they delete it from their device and re-install it, causing inconvenience and possible loss of data.



Responsible disclosure and protection

Check Point researchers responsibly disclosed their findings to Facebook and the Instagram team. Facebook's advisory was very responsive and helpful, they have described this vulnerability as an "Integer Overflow leading to Heap Buffer Overflow" and issued a patch to remediate the issue on the newer versions of the Instagram application on all platforms.

Facebook issued the following comment to accompany this research publication: "We've fixed the issue and haven't seen any evidence of abuse. We're thankful for Check Point's help in keeping Instagram safe."

The patch for this vulnerability has already been available for six months prior to this publication, giving time to the majority of users to update their Instagram applications, thus mitigating the risk of this vulnerability being exploited. Instagram users have been strongly encouraged to ensure they are using the latest Instagram app version and to update if any new version is available.