Instagram for Android

Overview

A vulnerability in the Android version of Instagram was recently discovered in versions prior to 120.0.0.26.128. In the affected versions, there is a vulnerability in the way Instagram processes images using "Mozjpeg", an open source tool used to decode JPEG images that are uploaded to its platform.

By exploiting this vulnerability, the attacker can take control of any function or permission Instagram has been granted by the user. For example, the attacker could control the device's microphone and camera or gain access to other data on the device that Instagram has permission to access. To commence an attack, the threat actor simply needs to send the target a malicious image, which could be through email, SMS, a 3rd-party messaging app, or another social media platform. If the target opens the malicious image in Instagram, the malicious code behind it is executed and the threat actor now has control of the target's Instagram app.

Lookout Analysis

In order for this attack to be successful, the victim needs to have a vulnerable version of Instagram installed, save the malicious image to the device, and then open it in Instagram. Since the malicious image can be delivered to the device in so many ways, a threat actor may be able to easily use social engineering to convince the target to upload the image. One particularly large risk is that many users automatically save images from WhatsApp, which takes the attacker one step closer to a successful attempt.

Once the attacker has control of Instagram's functionality, they could pose a massive security risk to the individual as well as the organization they work for if they choose to take control of the microphone and access data such as photos and contacts.

Lookout Coverage and Recommendation for Admins

Lookout will detect outdated versions of Instagram for Android as part of its default policy that alerts a user if an app on their device has an exploitable vulnerability. The admin can customize the policy to set a risk level and response that align with their organization's security policies.

If the admin chooses to alert devices, end users with vulnerable versions of the app will receive an alert from Lookout with instructions on how to update the app. The admin can also choose to block access to certain corporate domains or the internet altogether until the issue has been resolved.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Lookout Threat Advisory

© 2020 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ and DAY OF SHECURITY™ are trademarks of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.