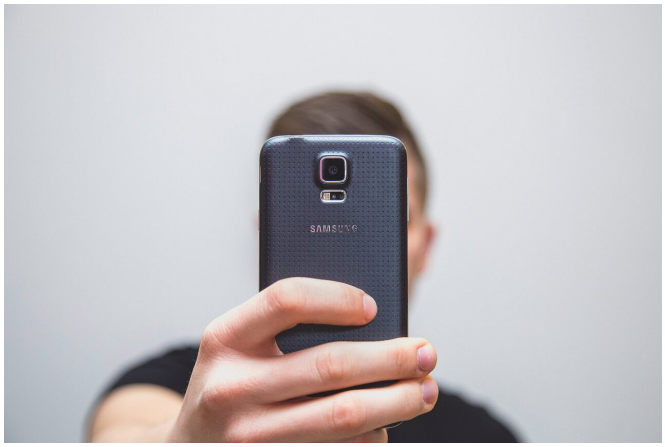
Team saw how an attacker could hijack Android camera for spyfest

20 November 2019, by Nancy Cohen



Credit: CC0 Public Domain

Android camera security threat, disclosed and since addressed, had spy vulnerabilities. These were fixed by Google and Samsung with a patch rolled out for Pixel and Samsung devices The recent headlines surrounding the flaw on Android devices teased a discomforting thought in the latest of numerous discomforting thoughts about security risks in the Android ecosystem.

Imagine your app is recording video and taking photos without your permission.

In short, attackers could hijack your phone camera. Dan Goodin in *Ars Technica*: This was all about "an app needed no permissions at all to cause the camera to shoot pictures and record video and audio."

What if your phone was locked? They could still do it. What if your screen was turned off? They could still do it.

On Tuesday, Erez Yalon, Director of Security Research at Checkmarx, opened up about the bugs, their team's attack strategy, and the vulnerabilities they discovered (CVE-2019-2234).

Meanwhile, *Security Affairs* on Tuesday introduced the issue to its readers, saying cybersecurity experts from Checkmarx discovered multiple vulnerabilities in the Android camera apps provided by Google and Samsung and these could have been exploited by hackers to spy on hundreds of millions of users.

"The vulnerabilities are collectively tracked as CVE-2019-2234, attackers could exploit them to conduct several activities, including recording videos, taking photos, recording voice calls, tracking the user's location."

As for the Checkmarx blog, Yalon detailed the path to discovery. "In order to better understand how smartphone cameras may be opening users up to privacy risks, the Checkmarx Security Research Team cracked into the applications themselves that control these cameras to identify potential abuse scenarios. The team has a Google Pixel 2 XL and Pixel 3 on-hand, ultimately finding multiple concerning vulnerabilities stemming from "permission bypass issues."

The team tested both versions of Pixel (2 XL / 3) in their labs. The team delivered a proof-of-concept (PoC) video and a technical report. Video notes said "The Checkmarx Security Research Team demonstrates how to exploit vulnerabilities found within the Google camera application, forcing the device to take photos, videos, and eavesdrop without the user's knowledge."

Yalon said the findings were shared with Google, Samsung and other Android-based smartphone OEMs.

Timeline from ZDNet: Google was informed of the researchers' findings on July 4. Google registered the CVE and confirmed that other vendors were impacted. A fix was released. Google said in a

statement. "The issue was addressed on impacted Google devices via a Play Store update to the Google Camera Application in July 2019. A patch has also been made available to all partners."

A Samsung spokesperson meanwhile told *Business Insider* the company also released patches to address the issue.

Alfred Ng in CNET reported that after Checkmarx informed Google and Samsung about the security issue in July. The two companies told Checkmarx they fixed the issue in a Play Store update the same month. However, Ng added, "While the patch is available, it's unclear if every affected device maker has issued the fix."

Dan Goodin in Ars Technica had a similar note of caution/ "Until recently, weaknesses in Android camera apps from Google and Samsung made it possible for rogue apps to record video and audio and take images and then upload them to an attacker-controlled server—without any permissions to do so. Camera apps from other manufacturers may still be susceptible."

Aaron Holmes*, Business Insider*, and Dan Goodin, *Ars Technica,* told their readers what to do to be safe not sorry: check your Android device, plain and simple, to see if it is vulnerable. They also suggested ways to check, if the device that needed checking was neither Pixel nor Samsuing, as Goodin noted that "camera apps from other manufacturers may still be susceptible."

APA citation: Team saw how an attacker could hijack Android camera for spyfest (2019, November 20) retrieved 28 November 2022 from https://techxplore.com/news/2019-11-team-hijack-android-camera-spyfest.html