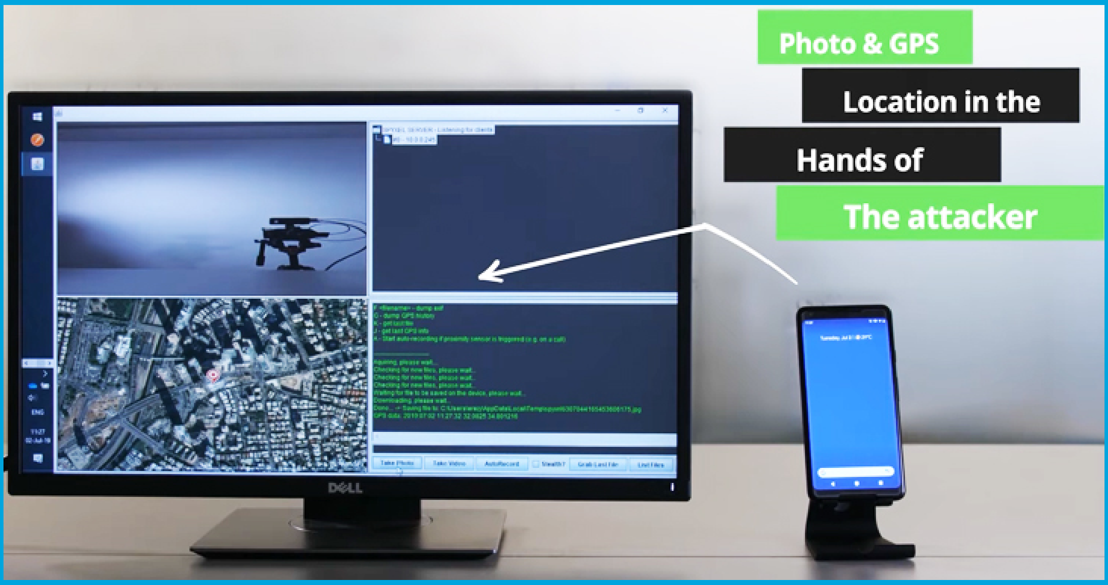
kindred

Security Newsletter

25 November 2019

Subscribe to this newsletter

New Flaw Lets Rogue Android Apps Access Camera Without Permission



An alarming security vulnerability has been discovered in several models of Android smartphones manufactured by Google, Samsung, and others that could allow malicious apps to secretly take pictures and record videos — even when they don't have specific device permissions to do so.

The attack scenario involves a rogue app that only needs access to device storage (i.e., SD card), which is one of the most common requested permissions and does not raise any suspicion. According to researchers, by merely manipulating specific "actions and intents," a malicious app can trick vulnerable camera apps into performing actions on behalf of the attacker, who can then steal photos and videos from the device storage after being taken. Since smartphone camera apps already have access to required permissions, the flaw could allow attackers to indirectly and surreptitiously take photos, record videos, eavesdrop on conversations, and track location — even if the phone is locked, the screen is off, or the app is closed.

The Checkmarx research team responsibly reported their findings to Google in early July with the PoC app and a video demonstrating an attack scenario. Google confirmed and addressed the vulnerability in its Pixel line of devices with a camera update that became available in July, and contacted other Android-based smartphone OEMs in late August to inform them about the issue, which the company rated as "High" in severity. However, Google did not disclose the names of the affected manufacturers and models.

Read More on TheHackerNews

Macy's Customer Payment Info Stolen in Magecart Data Breach

Macy's has announced that they have suffered a data breach due to their web site being hacked with malicious scripts that steal customer's payment information. This type of compromise is called MageCart attack and consists of hackers compromising a web site so that they can inject malicious JavaScript scripts into various sections of the web site. These scripts then steal payment information that is submitted by a customer.

According to a 'Notice of Data Breach' issued by Macy's, their web site was hacked on October 7th, 2019 and a malicious script was added to the 'Checkout' and 'My Wallet' pages. If any payment information was submitted on these pages while they were compromised, the credit card details and customer information was sent to a remote site under the attacker's control. As part of this breach, attackers were able to access customer information and credit card information that includes the customer's first name, last name, address, city, state,zip, phone number, email address, payment card number, payment card security code, and payment card month/year of expiration if submitted on a compromised page.

Macy's has started sending out emails to those who were affected and advise them to monitor their credit card statement for suspicious or fraudulent activity. If anything is detected, consumers should immediately contact their credit card company and dispute the charge. This isn't the first data breach notification to have been issued by Macy's. In June 2018, for example, Macy's notified customers that it had detected fraudulent attempts to use legitimate usernames and passwords to access customer accounts, also called Credential-Stuffing.

Read More on BankInfoSecurity

Even More on BleepingComputer

More #News

- T-Mobile Suffers Data Breach Affecting Prepaid Wireless Customers
- cuuBlock Origin Now Blocks Sneaky First-Party Trackers in Firefoxt2
- N26 Security 3.0
- Google offers up to $1.5 million bounty for remotely hacking Titan M chip
- Edenred Payment Solutions Giant Announces Malware Incident
- Card Skimmer Group Replaces Checkout Page to Steal Payment Info
- Microsoft Debunks Dopplepaymer Ransomware Rumors
- Undocumented Access Feature Exposes Siemens PLCs to Attacks
- Chrome, Edge, Safari hacked at elite Chinese hacking contest
- Black Friday Deals on the Dark Web: A cybercriminal shopper's paradise
- New GitHub Security Lab Aims to Secure Open Source Software
- Meet Phoenix Keylogger, a New Malware-as-a-Service Product Gaining Traction
- New Roboto botnet emerges targeting Linux servers running Webmin
- DDoS-for-Hire Boss Gets 13 Months Jail Time
- Official Monero Site Hacked to Distribute Cryptocurrency Stealing Malware
- Why Were the Russians So Set Against This Hacker Being Extradited?
- Compromised Website Led to Australia Parliament Hack
- Personal And Social Information Of 1.2 Billion People Discovered In Massive Data Leak from data enrichment firm

#Patch Time!

- Millions of Sites Exposed by Flaw in Jetpack WordPress Plugin
- Adobe announces end of support for Acrobat, Reader 2015
- Attackers using WhatsApp MP4 video files vulnerability can remotely execute code

#Tech and #Tools

- A Deep Dive On The Most Critical API Vulnerability — BOLA
- How to use CI/CD to deploy and configure AWS security services with Terraform
- Introducing Flan Scan: Cloudflare's Lightweight Network Vulnerability Scanner
- Security Checklist for Web Developers
- Continuously monitor unused IAM roles with AWS Config
- Sysmon Deep Dive Part 1: Process Create | Part 2: File Creation Time Changed
- The Internals of AppLocker - Part 1 - Overview and Setup | Part 2 - Blocking Process Creation
- How Google adopted BeyondCorp: Part 4 (services)
- Don't Get Kicked Out! A Tale of Rootkits and Other Backdoors
- My First SSRF Using DNS Rebinding
- Remote Code Execution via Struts devMode
- Cloud Network Security 101: AWS VPC Endpoints | AWS Security Groups vs NACLs
- Subdomain_recon.py: A SubDomain Reconnaissance Tool
- pdlist: A passive subdomain finder
- bounty-targets-data: hourly-updated data dumps of bug bounty platform scopes (like

Hackerone/Bugcrowd/etc) that are eligible for reports

- Genesis: framework to generate unique test cases based on code snippets to test techniques
- JavaFuzz: coverage guided fuzz testing for java
- Cracking reCAPTCHA, Turbo Intruder style
- Building up a basic Physical Red Team toolkit and skillset.
- Reasonably Secure Electron

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us