Security Newsletter

1 June 2020

Subscribe to this newsletter

New Android Flaw Affecting Over 1 Billion Phones Let Attackers Hijack Apps

A security vulnerability affecting Android that malicious apps can exploit to masquerade as any other app installed on a targeted device to display fake interfaces to the users, tricking them into giving away sensitive information. The same team of Norwegian cybersecurity researchers today unveiled details of a new critical vulnerability (CVE-2020-0096) affecting the Android operating system that could allow attackers to carry out a much more sophisticated version of Strandhogg attack.

Dubbed 'Strandhogg 2.0,' the new vulnerability affects all Android devices, except those running the latest version, Android Q / 10, of the mobile operating system—which, unfortunately, is running on only 15-20% of the total Android-powered devices, leaving billions of rest of the smartphones vulnerable to the attackers. However, unlike StrandHogg 1.0 that can only attack apps one at a time, the latest flaw could let attackers "dynamically attack nearly any app on a given device simultaneously at the touch of a button," all without requiring a pre-configuration for each targeted app

Security researchers responsibly reported the new vulnerability to Google in December last year. After that, Google prepared a patch and shared it with smartphone manufacturing companies in April 2020, who have now started rolling out software updates to their respective users from this month.

Read More on TheHackerNews

More #News

- Capital One Must Turn Over Mandiant's Forensics Report
- GitHub warns Java developers of new malware poisoning NetBeans projects
- Facebook Announces Messenger Security Features that Don't Compromise Privacy
- Fake Valorant Mobile app pushes scams on eager gamers
- 200K sites with buggy WordPress plugin exposed to wipe attacks
- Minted discloses data breach after 5M user records sold online
- Even tech-savvy Americans have bad online safety habits
- Researchers Uncover Brazilian Hacktivist's Identity Who Defaced Over 4800 Sites
- $100 million in bounties paid via HackerOne to ethical hackers
- Arbonne MLM data breach exposes user passwords, personal info
- New Octopus Scanner malware spreads via GitHub supply chain attack
- Cisco hacked by exploiting vulnerable SaltStack servers

#Patch Time!

- German govt urges iOS users to patch critical Mail app flaws
- Apple sends out 11 security alerts – get your fixes now!
- OpenSSH to deprecate SHA-1 logins due to security risk
- Docker Desktop danger discovered, patch now

#Tech and #Tools

- Phishing metrics - what to track?
- When Anti-Virus Engines Look Like Kernel Rootkits
- Sploitus. Vulnerability search engine
- Bypassing LastPass's "Advanced" YubiKey MFA: A MITM Phishing Attack
- step-by-step walkthrough of CloudGoat 2.0 scenarios.
- eBay is port scanning your system when you load the webpage
- These Aren't the Phish You're Looking For
- OSCP, CRTE … Which one should you take?
- Zero Trust Deployment Guide for devices

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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