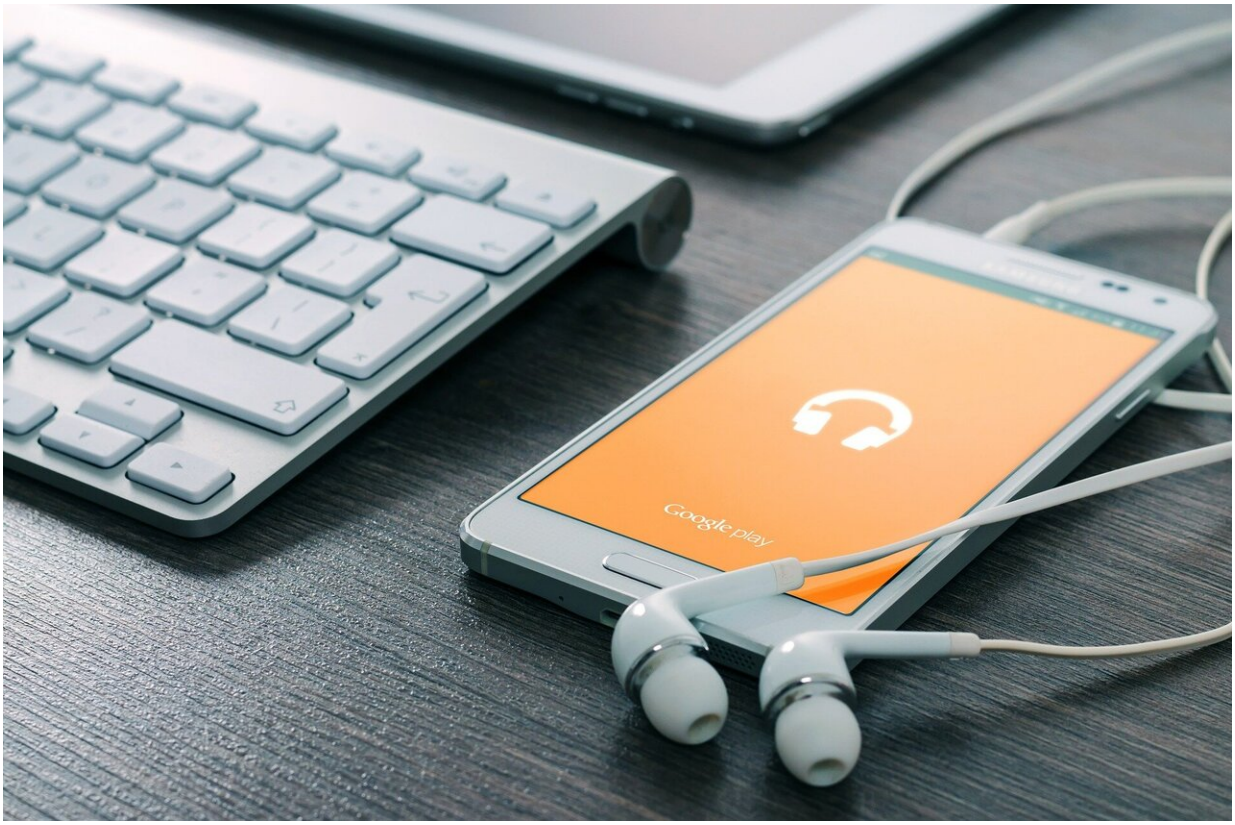
'Achilles' flaw exposes a billion Android phones

August 10 2020, by Peter Grad



Credit: CC0 Public Domain

One billion Android phones are at risk of attacks by hackers taking advantage of what a research firm says are 400 vulnerabilities detected on the smartphone's chips.

Collectively called "Achilles," the vulnerabilities were found on stretches of code found in Qualcomm's Snapdragon chips, which are found on nearly half of all Android phones.

Addressing the DEF CON Safe Mode security conference Friday, researchers at Check Point security firm said phones could be turned into spying tools providing access to photos, videos, location data, and other sensitive user details. The hacker need only successfully persuade a user to install a seemingly benign app that requires no permissions to operate.

Hackers could spy on phone conversations, launch denial-of-service attacks, or surreptitiously plant malicious code.

"You can be spied on. You can lose all your data," said said Yaniv Balmas, head of cyber research at Check Point. "If such vulnerabilities are found and used by malicious actors, it will find millions of mobile phone users with almost no way to protect themselves for a very long time."

Check Point has distributed details of its findings to Qualcomm and affected phone vendors. It did not post the details in public so as to not provide any advantages to hackers.

Qualcomm said it is addressing the vulnerabilities; issuing a new compiler and a new software development kit. But it is up to phone vendors to distribute patches for each model phone carrying the affected processor.

"For vendors, it means they will need to recompile each and every DSP application they use, test them, and fix any issues [that] may occur," said Balmas. "Then they need to ship these fixes to all devices in the market."

Snapdragon chipsets have been a welcome component of smartphones, wearable devices, and automobile systems. It's embraced for its speed and performance benchmarks, power efficiency, 5G support, graphics handling, and embedded fingerprint reading capacity.

Digital signal processors don't attract the same degree of scrutiny by researchers for possible flaws as other computer components because technical specs are usually closely guarded by manufacturers.

"While DSP chips provide a relatively economical solution that allows mobile phones to provide end users with more functionality and enable innovative features, they do come with a cost," researchers from Check Point state in a report posted online. "These chips introduce new attack surfaces and weak points to these mobile devices. DSP chips are much more vulnerable to risks as they are being managed as 'Black Boxes' since it can be very complex for anyone other than their manufacturer to review their design, functionality or code."

"Our research managed to break these limits and we were able to have a very close look at the chip's internal design and implementation in a relatively convenient way. Since such research is very rare, it can explain why we found so many vulnerable code sections," Balmas said.

Snapdragon system-on-a-chip products can be found on leading phone products by Google, Samsung, Xiaomi, LG, and OnePlus. Apple provides its own processors, so iPhones are not affected by Achilles.

Qualcomm said it has no evidence the vulnerabilities are "currently being exploited," but urged customers "to update their devices as patches become available and to only install applications from trusted locations, such as the Google Play Store."

More information: www.defcon.org/html/defcon-saf …

akers.html#Makkaveev