1. Android Security vulnerabilities — February 2019

A recently discovered critical vulnerabilities in Android OS leaves it open to the remote code execution attack. As published on [https://goo.gl/6SxVYy] the three critical vulnerabilities CVE-2019-1986, CVE-2019-1987 and CVE-2019-1988 can expose the entry for an attacker to remotely execute code with higher privilege.

The bug exists in the OSs module that renders PNG files. As google has pushed the security update to source project mentions fixing “buffer overflow flaw” in “errors in SkPngCodec”. The vulnerability exists in the Android OS's framework and gets triggered as soon as the user opens the PNG file. The vulnerability affects the Android devices ranging from Android 7.0 to Android 9.0.

A cleverly manipulated PNG (Portable Network Graphics) image file, could execute arbitrary code on the device within the context of a privileged process, Moreover, the attacker could send the file through any client like instant messaging client or mobile email.

Why is this significant:

- Given the fragmented nature of Android it is very unlikely that many manufactures would push the fix so early onto the devices. As many devices remain unpatched, the impact this could have is huge.
- The widespread use of Android devices (over 2 billion monthly active devices [1]), leaves many individuals vulnerable to the attack.

Another interesting read I found is below.

2. Remote Code Execution in apt/apt-get

As discovered by Max Justicz in his blog [https://goo.gl/R1Pmph]a vulnerability in apt package manager allows a man-in-the-middle attack on network to run any code with highest privilege i.e. root while one is installing the any package.

As shown by the researcher in the blogpost an attacker intercepting HTTP traffic between APT and mirror servers, can inject malicious code/package into the traffic and execute the code with root privileges. The APT utility doesn't properly sanitize certain parameters during HTTP redirects, allowing man-in-the-middle attackers to inject malicious content.

Why is this significant:

This shows the adaptation and support of https for open-source projects or for any project for that matter should be designed form first.