[GitHub - aosp-mirror/platform\_build](https://github.com/aosp-mirror/platform_build)

<https://cs.android.com/android>

Android Verson 5.10 and 5.15

Summary of Work:

The WPT Group viewed and analyzed the above files in search of how the Android operating system interacts and interprets, if at all, any incoming Qi communications. This is a field that we were unable to find already published information for, so we began exploring each aspect of the operating system source code.

Current theories on this interaction are that it is either very limited within the OS or that the installed Qi receiver operates primarily as a hardware component with its own microcontroller requiring minimal OS oversight and interaction. This theory is based on the collected information and interpretation of receiver standards from the following documents: <https://ieeexplore.ieee.org/document/6099840>, Demodulating Communication Signals of Qi-Compliant Low-Power Wireless Charger Using MC56F8006 DSC by: Xiang Gao, and <https://www.mdpi.com/1424-8220/22/15/5573/pdf?version=1658829347>. While we acknowledge that Apple can turn Qi WPT on and off via system settings, without access to the source code we cannot determine the nature by which the OS interacts with the process and would assume that Apple devices also follow the theory proposed earlier.

During our investigation into the Android OS specifically, we found no evidence to suggest that the OS controls the process overtly (besides normal battery function and recognizing that the phone is receiving power). This could be due to our lack of expertise in reading and understanding the very complicated source code, however we do believe that our findings give us enough of a confirmation as to our original hypothesis in order to conclude that this vector is not a real possibility for this group to pursue. The potential for OS interaction to a meaningful degree from what we have seen is unlikely to be anything more than severely limited. We believe the best vector for attack using this technology will remain as voltage analysis (side channel attacks using voltage) and as denial-of-service style attacks using injection methods.

Presently, we have concluded research in this area, the time it would require to find the specific way Qi is interpreted is not viewed as being worth what this finding would provide in the overall research.