The new attack technique uses a wireless charger to issue voice commands and heat up the device

Researchers at the University of Florida and CertiK discovered a new series of attacks called 'VoltSchemer' that can use the magnetic field emitted from a wireless charger to issue voice commands that control the phone's voice assistant. smart phone.

Based on the principle of electromagnetic induction, wireless charging systems often use electromagnetic fields to transfer energy between two objects. The charging station contains a transmitter coil, through which alternating current flows to create an oscillating magnetic field. Smartphones contain a coil that collects energy from the magnetic field and converts it into electrical energy to charge the battery.

Attackers can exploit security vulnerabilities in the hardware design of wireless charging systems and the protocols that manage their communications to manipulate and fine-tune the voltage delivered on the input. of the charger, creating an interference signal that can interfere with the periodic exchange of data between the charging station and the smartphone, 'distorting' the power signal and corrupting highly accurate transmitted data.

This allows hackers to perform VoltSchemer attacks for the purpose of overheating/overcharging, bypassing Qi safety standards.

When the battery is fully charged, the smartphone will stop charging. The interference signal introduced by VoltSchemer can interfere with operation, causing the smartphone to continue charging when the battery is full leading to overcharging and overheating, posing a significant hazard.

The VoltSchemer attack can also bypass Qi standard safety mechanisms to initiate power transfer to nearby unsupported devices such as car keys, USB cards, RFID chips, SSD drives in computers. portable. causing overheating and damage.

The researchers disclosed their findings to charging station vendors in search of countermeasures that would eliminate the risk of a VoltSchemer attack.