Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks

Vendor: Tesla, Inc.
Vendor URL: https://www.tesla.com
Versions affected: Attack tested with vehicle software v11.0 (2022.8.2 383989fadeea) and iOS app 4.6.1-891 (3784eb63).
Systems Affected: Attack tested on Model 3. Model Y is likely also affected.
Author: Sultan Qasim Khan <sultan.qasimkhan[at]nccgroup[dot]com>
Risk: <6.8 CVSS v3.1 AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N> An attacker within Bluetooth signal range of a mobile device configured for Phone-as-a-Key use can conduct a relay attack to unlock and operate a vehicle despite the authorized mobile device being out of range of the vehicle.

https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/
Experts show how to run malware on chips of a turned-off iPhone

May 16, 2022 By Pierluigi Paganini

Researchers devised an attack technique to tamper the firmware and execute a malware onto a Bluetooth chip when an iPhone is “off.”

A team of researchers from the Secure Mobile Networking Lab (SEEMOO) at the Technical University of Darmstadt demonstrated a technique to tamper with the firmware and load malware onto a chip while an iPhone is “OFF.”

Experts pointed out that when an iPhone is turned off, most wireless chips (Bluetooth, Near Field Communication (NFC), and Ultra-wideband (UWB)) continue to operate.

The Bluetooth and UWB chips are hardwired to the Secure Element (SE) in the NFC chip, storing secrets that should be available in LPM,” the researchers said.

The Low-Power Mode was implements with iOS 15, it is supported by iPhone 11, iPhone 12, and iPhone 13 devices.

https://securityaffairs.co/wordpress/131336/hacking/malware-execution-iphone-turned-off.html