Michael Esposito

Network Defense 2

Vulnerabilities in Apple’s bluetoothd daemon

**CVE-2018-4087**

This vulnerability lies inside the Bluetooth daemon running on tvOS, iOS, and watchOS. It leads to the execution of arbitrary code on different crucial daemons in iOS by hijacking the session between each daemon and bluetoothd. It was discovered in October of 2017, confirmed by Apple in December, and patched in January 2018. The details of this vulnerability were published last week, and Apple was able to path the vulnerability quickly.

**Attack Process**

When a legitimate client is attempting to make a session with bluetoothd, it is given a session token once it successfully joins. These session tokens were given out using a predicable schema, and the inter-process communication (IPC) port of other high-level processes could be brute forced. In theory, with knowledge of the IPC ports of these other processes an attacker could escape the tight sandbox environment on an Apple device. The sandbox is one of the prided features of Apple devices, so the ability of expanding this attack service is a pretty incredible discovery.

**Affected Processes**

* SpringBoard
* mDNSResponder
* aggregated
* wifid
* Preferences
* CommCenter
* iaptransportd
* findmydeviced
* routined
* UserEventAgent
* carkitd
* mediaserverd
* bluetoothd
* coreduetd