[Presentation] Why You Should Leave Your Smart Grill Unplugged ?

written by Mert SARICA | 2 October 2023
You can access the presentation file (PDF) on my Why You Should Leave Your Smart Grill Unplugged ? presentation that I held at the BSidesNoVA conference by clicking this link here.

Abstract

As of 2023, approximately ~8 billion humans on our planet and 16 billion connected IoT devices equivalent to twice the total number of humans. IoTs are everywhere, from fish tanks to thermostats, toilets to belts, and even grills.

Unfortunately, many of them have severe weaknesses due to their limited hardware and software capabilities and are waiting to be discovered by cybersecurity researchers to be fixed by the manufacturers.

According to statistics, as of the beginning of 2021, 100 million households in America were using grills. We can predict that the widespread use of smart grills (IoT) will bring serious security risks.

In this presentation, I will explain how I hacked my Bluetooth Low Energy enabled, Mongoose OS-based smart grill by sending commands via BLE to obtain my home wireless network name (SSID) and password that I entered during the setup process of the grill.

Surprisingly, it is possible to exploit the vulnerability if the grill is not turned on (POWER ON) and only plugged in.

Physical Prerequisite:
Depending on the BLE transmitter, the attacker must locate himself 98 to 984 feet away from the grill.

Presentation Outline

1. Introduction to key terms and statistics (IoT, BLE, statistics…)
– This will detail the basic terminology and statistics

2. Fictional storytelling based on APT 28’s campaign
– Threat actors, APT groups might come after you even in physical world.

3. Vulnerability Discovery
– Reversing the mobile app of the grill
– Analyzing the BLE packets between the mobile app and the smart grill with tools and techniques.
– Understanding the fundamental of the communication
– Discovering the operating system running on the grill and functions that lead to vulnerability

4. Exploitation
– How to use a USB Bluetooth device and basic tools to exploit the vulnerability and obtaining the WiFi SSID and password.

5. Closing Remarks
– Finally the mitigation, cook, eat, enjoy and leave your grill unplugged or do not use the smart features.

Attendee Takeaways Notes

1. Even grills are getting smarter and depending on my assumption, in near future there will be no choice to find out and purchase a new, non smart (iot) devices. Keep monitoring your home network against malicious activity and harden your internal systems and devices. (Protection, Awareness)

2. If it is applicable and not required, do not enroll your IoT devices to your home network otherwise use guest network. (Mitigation, Awareness)

3. Beware of IoT vulnerabilities, aware of security risks and do not underestimate. (Awareness)