METMOX

Delivering values innovatively

The dark side of smart lights!

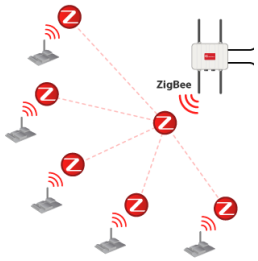
Flaw in Philips Smart Light Bulbs

Home automation although not common yet is a very fascinating technology. Taking our comfort to the next level, it means controlling the fans, bulbs, doors and more with just one click. However, this also means lesser security with the increasing edge of simplicity. This was confirmed lately when Philips Hue Smart Light Bulbs were found to be vulnerable to cyber-attacks.

Smart light bulbs and it's functioning

The concept of IoT is well known, but how many of us have heard of smart lightbulbs? By using a mobile app, or digital home assistant, we can control the lights in our house and even calibrate the colour of each lightbulb! With a wide range of 256 colour options. Smart isn't it?

These smart lightbulbs are functioned over the air using the familiar Wifi protocol or ZigBee, a low bandwidth radio protocol.



Zigbee

In recent times, we have seen how hundreds of widely used smart-but-insecure devices made it easier for remote attackers to sneak into connected networks without breaking WIFI passwords.

Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless mesh IoT networks and primarily used for two-way communication between a sensor and a control system. It is a short-range communication like Bluetooth and Wi-Fi offering connectivity up to 100 meters. The Zigbee protocol is stable, which is one of the reasons why it has become one of the world's most widely adopted protocols.

Philips implemented the Zigbee communication protocol in its 'hue smart light bulb' and security experts discovered a high-severity flaw in that which can be exploited by hackers to enter a targeted Wifi network. From this exploitation, the attacker can infiltrate home or office networks over the air spreading ransomware or spyware.

The attack Scenario

- According to the security researchers, the vulnerability could allow a local attacker/hacker to take control of Hue light bulbs using a malicious over-the-air update.
- Buffer overflow happens on a component called the "bridge" that accepts remote commands sent to the bulb over Zigbee protocol from other devices like a mobile app or Alexa home assistant.
- The hacker controls the bulb's colour or brightness to trick users into thinking the bulb has a glitch and eventually causes the bulbs to exhibit random behaviour and become uncontrollable/unreachable to operate.
- Then the user must delete the bulb (as the only way to reset the bulb is to delete it from the app and re-install) and then instruct the control bridge to re-discover the bulb.
- The bridge discovers the compromised bulb(The catch here is that the bulb discovered after re-installation is a malicious one and not the user's original which means in the process of rediscovering the attacker gain access to it) and the user adds it back onto their network.
- The hacker-controlled bulb with updated firmware then uses the ZigBee protocol vulnerabilities to trigger a heap-based buffer overflow on the control bridge, by sending a large amount of data to it. This data enables the hacker to install malware on the bridge – which is in turn connected to the target business or home network.
- The malware connects back to the hacker using a known exploit (such as Eternal Blue), they can infiltrate the target IP network from the bridge and can be used for different purposes like spread ransomware or spyware or simple viruses or remotely hack other devices connected to the same network

Patch information

Philips Hue brand owner in November 2019. Signify confirmed the existence of the vulnerability in their product, and issued a patched firmware version (Firmware 1935144040) which is now available on their site (https://www2.meethue.com/en-us/support/release-notes/bridge)

Recommendations

The automatic firmware update download feature is not enabled then it needs to manually install patches and change settings to revive future updates automatically.

"I think it's a very big problem, not just with the specific attack we've shown with the lights. We should speak about how we do security in IoT," Ronen said to Forbes. "The main issue [in the lightbulbs] is that there are not enough security measures."

The gist of this is that the companies focusing on IoT solutions need to exert more effort on security standards. Also, it is imperative to ensure the security of their products as a lot is at stake if an attacker finds a loophole like they always do. So, if one of your Hue bulbs starts malfunctioning, flickering or looks suspicious, do not risk your business or home networks and data without security systems. After all, technology is developed to help, not to destroy.