Your Philips Hue light bulbs can still be hacked] —and until recently, compromise your network.

Might want to check if you've got firmware 1935144040
By Sean Hollister

Feb 5, 2020, 6:00am EST

Four years ago, security researchers showed how a flying drone could hack an entire room full of Philips Hue smart light bulbs from *outside* a building, by setting off a virus- like chain reaction that jumped from bulb to bulb. Today, we're learning that vulnerability never got fully fixed — and now, researchers have figured out a way to exploit that very same issue to potentially infiltrate your home or corporate network, unless you install a patch.

That's the word from cybersecurity research firm Check Point Software, and the good news is you should *already* be safe from the worst part of the hack. If the Philips Hue Hub that controls your bulbs is connected to the internet, it should have automatically updated itself to version 1935144040 by now, which contains the patch you want.

(Check Point informed Philips in November, and a patch was issued mid-January.) I just checked my own hub's firmware version in the Philips Hue app, and I'm good.

https://www.theverge.com/2020/2/5/21123491/philips-hue-bulb-hack-hub-firmware-patch-update

It's also nice to know it might have taken a fairly clever, patient hacker to exploit this vulnerability in the first place. In addition to presumably uploading a malicious over-the- air update to a Hue bulb (the technique used in 2016), it relies on messing with that hacked bulb's color and brightness long enough to trick the owner into resetting and adding that bulb to their own network, at which point the hacked bulb overwhelms

the Hue Hub with data, taking control of the Hub in turn. Here's how Check Point explains that part:

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 also enables the hacker to install malware on the bridge –which is in turn connected to the target business or home network.

But it appears that once again, the bulbs *themselves* may still be vulnerable to hacks. When that flying drone set off a miniature IoT virus in 2016, companies found a way to solve for that worst-case scenario by restricting those bulb-to-bulb hops, writes Check Point. But “due to design limitations”, the bulb’s vulnerability remained, leading to the new hack — and perhaps other yet-to-be-discovered hacks in our future, as long as these bulbs remain in service. Leaving these bulbs vulnerable might be more dangerous than simply letting a hacker flick on and off your lights at will.

And though Check Point hasn’t necessarily tested other brands yet, its researchers claim this vulnerability may not be limited to Philips Hue bulbs and hubs. It’s in the Zigbee communications protocol used by loads of smart home brands, including Amazon’s Ring, Samsung SmartThings, Ikea Tradfri, Belkin’s WeMo, as well as Yale locks, Honeywell thermostats, and Comcast’s Xfinity Home alarm system.

It’s going to be interesting to see how many of the devices homeowners and businesses have purchased — ones they presumably expect to last for years — might open them up to security vulnerabilities years down the road. And we’re still wondering when the next massive IoT botnet built from insecure gadgets might rear its ugly head, as well.