Investigadores de Check Point revelaron hoy una nueva vulnerabilidad grave que afecta a las bombillas inteligentes Philips Hue, que se puede explotar desde más de 100 metros de distancia para acceder a una red WiFi específica.

La vulnerabilidad subyacente de alta gravedad, rastreada como CVE-2020-6007, reside en la forma en que Philips implementó el protocolo de comunicación Zigbee en su bombilla inteligente, lo que lleva a un problema de desbordamiento de búfer.

ZigBee es una tecnología inalámbrica ampliamente utilizada diseñada para permitir que cada dispositivo se comunique con cualquier otro dispositivo en la red. El protocolo se incorporó a decenas de millones de dispositivos en todo el mundo, incluyendo Amazon Echo, Samsung SmartThings, Belkin Emo y más.

> *«A través de esta explotación, un actor de amenazas puede infiltrarse en la red informática de una casa u oficina por el aire, propagando ransomware o spyware, utilizando nada más que una computadora portátil y una antena de más de 100 metros»*, dijeron los investigadores a THN.

Check Point también confirmó que el desbordamiento del búfer ocurre en un componente llamado «bridge» que acepta comandos remotos enviados a la bombilla por medio del protocolo Zigbee desde otros dispositivos, como una aplicación móvil o un asistente doméstico Alexa.

Aunque los investigadores no revelaron detalles técnicos completos o un código de prueba de concepto, compartieron un video que demuestra el ataque.

Según el video, el escenario de ataque implica:

- Al explotar un error previamente descubierto, un atacante primero toma el control de la bombilla inteligente.
- Con esto, se logra que el dispositivo sea *«inalcanzable»* en la aplicación de control de

los usuarios, engañándolos para que reinicien la bombilla y luego indique al puente de control que vuelva a descubrir la bombilla.
- El puente descubre la bombilla controlada por hackers con firmware actualizado, el usuario la vuelve a agregar a su red.
- El hacker explota las vulnerabilidades del protocolo ZigBee para desencadenar un desbordamiento de búfer basado en el puente de control, lo que le permite instalar malware en el puente que está conectado a la red objetivo.
- El hacker puede usar malware para infiltrarse en la red, dejando eventualmente millones de otros dispositivos conectados a la misma red en riesgo de piratería remota.

> *«Muchos de nosotros somos conscientes de que los dispositivos de IoT pueden suponer un riesgo de seguridad, pero esta investigación muestra cómo incluso los dispositivos más mundanos y aparentemente 'tontos', como las bombillas, pueden ser explotados por piratas informáticos y utilizados para apoderarse de redes o plantar malware»*, dijo Yaniv Balmas, jefe de investigación cibernética en Check Point.

Check Point informó de forma responsable estas vulnerabilidades a Philips y Signify, propietario de la marca Philips Hue, en noviembre de 2019, y el mes pasado la compañía lanzó un firmware actualizado y parcheado para el dispositivo.

> *«Es fundamental que las organizaciones y los individuos se protejan contra estos posibles ataques actualizando sus dispositivos con los últimos parches y separándolos de otras máquinas en sus redes, para limitar la posible propagación de malware. En el complejo panorama de ciberataques de hoy en día, no podemos darnos el lujo de pasar por alto la seguridad de cualquier cosa que esté conectada a nuestras redes».*

Si la función de descarga automática de actualizaciones de firmware no está habilitada, se recomienda a los usuarios afectados que instalen manualmente los parches y cambien la configuración para aprovechar futuras actualizaciones de forma automática.