Un investigador de seguridad cibernética recibió una recompensa por informar vulnerabilidades de $107,500 dólares, por haber identificado problemas de seguridad en los parlantes de Google Home, que podrían explotarse para instalar puertas traseras y convertirlas en dispositivos de escucha telefónica.

Las vulnerabilidades *«permitieron que un atacante dentro de la proximidad inalámbrica instalara una cuenta de 'puerta trasera' en el dispositivo, lo que les permitía enviar comandos de forma remota a través de Internet, acceder a la alimentación del micrófono y realizar solicitudes HTTP arbitrarias dentro de la LAN de la víctima»,* dijo el investigador Matt.

Al realizar dichas solicitudes maliciosas, no solo podría quedar expuesta la contraseña de WiFi, sino que también proporcionaría al adversario acceso directo a otros dispositivos conectados a la misma red. Después de la divulgación responsable el 8 de enero de 2021, Google solucionó los problemas en abril de 2021.

El problema, en otras palabras, tiene que ver con cómo se puede aprovechar la arquitectura del software Google Home para agrega una cuenta de usuario de Google no autorizada al dispositivo de automatización del hogar de un objetivo.

En una cadena de ataque detallada por el investigador, un atacante que busca espiar a una víctima puede engañar a la persona para que instale una aplicación de Android maliciosa que, al detectar un dispositivo Google Home en la red, emite solicitudes HTTP sigilosas para vincular la cuenta de un atacante al dispositivo de la víctima.

Llevando las cosas un poco más arriba, también surgió que, al organizar un ataque de desautenticación de WiFi para obligar a un dispositivo Google Home a desconectarse de la red, se puede hacer que el dispositivo ingrese en un *«modo de configuración»* y cree su propio WiFi abierto.

El atacante puede conectarse posteriormente a la red de configuración del dispositivo y solicitar detalles como el nombre del dispositivo, cloud_device_id y certificado, y utilizarlos para vincular su cuenta al dispositivo.

Independientemente de la secuencia de ataque empleada, un proceso de enlace exitoso permite al adversario aprovechar las rutinas de Google Home para bajar el volumen a cero y llamar a un número de teléfono específico en cualquier momento para espiar a la víctima por medio del micrófono del dispositivo.

> *«Lo único que la víctima puede notar es que los LED del dispositivo se vuelven azules fijos, pero probablemente supongan que está actualizando el firmware o algo así. Durante una llamada, los LED no parpadean como lo hacen normalmente cuando el dispositivo está escuchando, por lo que no hay indicación de que el micrófono esté abierto»,* dijo Matt.

Además, el ataque puede extenderse para realizar solicitudes HTTP arbitrarias dentro de la red de la víctima e incluso leer archivos o introducir modificaciones maliciosas en el dispositivo vinculado que se aplicarían después de un reinicio.

Esta no es la primera vez que se diseñan métodos de ataque de este tipo para husmear de forma encubierta en objetivos potenciales por medio de dispositivos activados por voz.