Un equipo de investigadores de seguridad de Microsoft descubrió una vulnerabilidad crítica en la versión compatible con Bluetooth de las Google Titan Security Keys, que no se pudo reparar con una actualización de software.

Sin embargo, los usuarios no tiene por qué preocuparse, pues Google anunció que ofrecerá un reemplazo gratuito para los dongles Titan Sexurity Key.

En un aviso de seguridad publicado el miércoles, Google informó que una *«mala configuración en los protocolos de emparejamiento de Bluetooth de Titan Security Keys»* podría permitir que un atacante físicamente cerca de su clave de seguridad (unos 30 pies), se comunique con él o con el dispositivo en el que se encuentra su clave.

Titan Security Key fue lanzado por Google en agosto del año pasado, siendo un dispositivo USB de bajo costo que ofrece autenticación de dos factores basada en hardware para cuentas en línea con el nivel más alto de protección contra ataques de phishing.

Se vende en 50 dólares en la tienda de Google e incluye dos claves: una clave de seguridad USB-A con NFC y una clave Bluetooth/NFC equipada con batería y con Micro-USB para la autenticación segura de dos factores.

Según Google, la vulnerabilidad solo afecta a la versión BKE de las Titan Security Key, que tienen un signo T1 o T2 en la parte posterior, y otras claves de seguridad que no son Bluetooth, versiones compatibles con USB o NFC, son seguras para utilizar.

Christian Brand, Manager de Google Cloud Product describió los siguientes escenarios de ataque:

> *«Cuando intentas iniciar sesión en una cuenta en tu dispositivo, normalmente se pide que presiones el botón en tu BLE para activarlo. Un atacante que se encuentre cerca en ese momento puede potencialmente conectar su propio dispositivo a tu Titan Security Key afectada antes de que tu propio dispositivo se conecte. En este*

> *conjunto de circunstancias, el atacante podría iniciar sesión en tu cuenta con tu propio dispositivo si el atacante de alguna manera ya obtuvo tu nombre de usuario y contraseña».*
>
> *«Antes de que puedas utilizar tu clave de seguridad, debe emparejarse con tu dispositivo. Una vez emparejado, un atacante que esté cerca podría utilizar tu dispositivo para hacerse pasar por tu Titan afectado y conectarse al dispositivo en el momento que se le solicite para presionar el botón. Después de eso, podrían intentar cambiar el dispositivo para que aparezca como un teclado o mouse Bluetooth y posiblemente tomar medidas en tu dispositivo».*

Microsoft descubrió la vulnerabilidad y la reveló a Google, así como a Feitian, la compañía que fabrica Titan Keys para Google y también vende el mismo producto (ePass) bajo su propia marca.

Feitian también hizo una divulgación coordinada sobre la vulnerabilidad el mismo día que Google estaba ofreciendo un programa de reemplazo gratuito para sus usuarios.

Como el problema solo afecta al protocolo de emparejamiento de baja energía de Bluetooth y no a la seguridad criptográfica de la clave en si, Google recomienda a los usuarios afectados que sigan utilizando sus claves existentes hasta que obtengan un reemplazo.

Google también asegura que la clave de seguridad de Bluetooth es aún más segura que apagarla por completo o confiar en otros métodos de autenticación de dos factores como SMS o llamadas telefónicas.

Sin embargo, sería mejor si tomas algunas medidas adicionales al utilizar las claves de seguridad, como usarlas solo en un lugar privado y desemparejarlas inmediatamente.