Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Advisory: Security Issue with Bluetooth Low Energy (BLE) Titan Security Keys

May 15, 2019

Posted by Christiaan Brand, Product Manager, Google Cloud

We've become aware of an issue that affects the Bluetooth Low Energy (BLE) version of the Titan Security Key available in the U.S. and are providing users with the immediate steps they need to take to protect themselves and to receive a free replacement key. This bug affects Bluetooth pairing only, so non-Bluetooth security keys are not affected. Current users of Bluetooth Titan Security Keys should continue to use their existing keys while waiting for a replacement, since security keys provide the strongest protection against phishing.

What is the security issue?

Due to a misconfiguration in the Titan Security Keys' Bluetooth pairing protocols, it is possible for an attacker who is physically close to you at the moment you use your security key -- within approximately 30 feet -- to (a) communicate with your security key, or (b) communicate with the device to which your key is paired. In order for the misconfiguration to

be exploited, an attacker would have to align a series of events in close coordination:

- When you're trying to sign into an account on your device, you are normally asked to press the button on your BLE security key to activate it. An attacker in close physical proximity at that moment in time can potentially connect their own device to your affected security key before your own device connects. In this set of circumstances, the attacker could sign into your account using their own device if the attacker somehow already obtained your username and password and could time these events exactly.
- Before you can use your security key, it must be paired to your device. Once paired, an attacker in close physical proximity to you could use their device to masquerade as your affected security key and connect to your device at the moment you are asked to press the button on your key. After that, they could attempt to change their device to appear as a Bluetooth keyboard or mouse and potentially take actions on your device.

This security issue does not affect the primary purpose of security keys, which is to protect you against phishing by a remote attacker. Security keys remain the strongest available protection against phishing; it is still safer to use a key that has this issue, rather than turning off security key-based two-step verification (2SV) on your Google Account or downgrading to less phishing-resistant methods (e.g. SMS codes or prompts sent to your device). This local proximity Bluetooth issue does not affect USB or NFC security keys.

Am I affected?

This issue affects the BLE version of Titan Security Keys. To determine if your key is affected, check the back of the key. If it has a “T1” or “T2” on the back of the key, your key is affected by the issue and is eligible for free replacement.

Steps to protect yourself

If you want to minimize the remaining risk until you receive your replacement keys, you can perform the following additional steps:

iOS devices:

On devices running iOS version 12.2 or earlier, we recommend using your affected security key in a private place where a potential attacker is not within close physical proximity (approximately 30 feet). After you’ve used your key to sign into your Google Account on your device, immediately unpair it. You can use your key in this manner again while waiting for your replacement, until you update to iOS 12.3.

Once you update to iOS 12.3, your affected security key will no longer

work. You will not be able to use your affected key to sign into your Google Account, or any other account protected by the key, and you will need to order a replacement key. If you are already signed into your Google Account on your iOS device, do not sign out because you won't be able to sign in again until you get a new key. If you are locked out of your Google Account on your iOS device before your replacement key arrives, see these instructions for getting back into your account. Note that you can continue to sign into your Google Account on non-iOS devices.

On Android and other devices:

We recommend using your affected security key in a private place where a potential attacker is not within close physical proximity (approximately 30 feet). After you've used your affected security key to sign into your Google Account, immediately unpair it. Android devices updated with the upcoming June 2019 Security Patch Level (SPL) and beyond will automatically unpair affected Bluetooth devices, so you won't need to unpair manually. You can also continue to use your USB or NFC security keys, which are supported on Android and not affected by this issue.

How to get a replacement key

We recommend that everyone with an affected BLE Titan Security Key get a free replacement by visiting google.com/replacemykey.

Is it still safe to use my affected BLE Titan Security Key?

It is much safer to use the affected key instead of no key at all. Security keys are the strongest protection against phishing currently available.

No comments :

Post a Comment

Links to this post

Create a Link