The newly released macOS has detected a serious security vulnerability

Newly released to the public today as Apple's latest MacOS High Sierra operating system has an important security hole, allowing hackers to access Plainted Keychain Data.

Newly released to the public today as Apple's latest MacOS High Sierra operating system has an important security hole, allowing hackers to access Plainted Keychain Data.

Unregistered applications on macOS High Sierra (and possibly the previous version of macOS) can steal usernames and account passwords stored on Keychain.

Security researcher and former NSA analyst Patrick Wardle talked about this vulnerability and shared a video of how to exploit it.

In order for this vulnerability to work, users need to download third-party malicious code from an unknown source, Apple often discourages users from downloading applications from untrusted developers or from outside the Mac App Store. . Apple does not even allow downloading from untrusted developers without overwriting security settings.

In the video illustrated, Wardle creates a POC application called keychainStealer that can access the plaintext passwords of Twitter, Facebook and Bank of America stored on Keychain.

An attacker can steal data on Plaintext Keychain

Wardle told Forbes about the vulnerability and said it was not too difficult to run malicious code on the Mac even with Apple's protection. Wardle does not provide the entire exploit code, but he also believes Apple will fix the vulnerability in the next update.

Apple has not responded when asked about this vulnerability.