Issued 9/28/17

Nasty Password-Pilfering Hack Ruins Apple macOS High Sierra Launch

Apple released a new macOS operating system today, dubbed High Sierra. But already a serious weakness has been found lurking within, a security researcher has claimed, allowing a hacker to steal passwords from Apple Macs running the new OS. Patrick Wardle, ex-NSA analyst and now head of research at security firm Synack, found the problem Monday, warning that it could allow anyone able to run malicious code on a Mac to pilfer passwords from the keychain.

Apple uses the keychain to store user passwords and should only be accessible to the owner of the Mac. All those logins are typically unlocked with a master password. But Wardle, as shown in the video below, was able to carry out an attack that sent all the contents of the keychain to an attacker without the need for that password. With his "keychainStealer" app, the researcher's hack forced the keychain to disclose Facebook, Twitter and Bank of America passwords. Also note Wardle's cheeky request for a macOS bug bounty for charity during the launch process for the keychainStealer. "Without root priveleges, if the user is logged in, I can dump and exfiltrate the keychain, including plaintext passwords," Wardle told Forbes. "Normally you are not supposed to be able do that programmatically."

At the time of publication, Apple hadn't responded to a request for comment.