Issued 5/11/17

Vulnerability Allowed Hackers to Steal iCloud Keychain Secrets

Apple has recently patched a Keychain vulnerability that could have been exploited by man-in-the-middle (MitM) attackers to obtain sensitive user information. The details of the flaw were disclosed on Monday by the researcher who reported it to the vendor.

One of the many security holes **patched by Apple** in late March in iOS, macOS and other products is CVE-2017-2448, a Keychain weakness discovered by Alex Radocea of Longterm Security. According to Radocea, the flaw affects the iCloud Keychain, which stores account names, passwords, credit card data, and Wi-Fi network information. The iCloud Keychain sync feature allows users to synchronize their keychain so that passwords and other data are accessible from all their Apple devices. Apple designed the iCloud Keychain to be highly secure and it told customers that **not even the NSA can access their secrets**. The sync feature uses end-to-end encryption to exchange data — the encryption relies on a syncing identity key unique to each device, and the encryption keys are never exposed to iCloud.

Data is transmitted via the iCloud Key-Value Store (KVS), which applications use to synchronize the data of iCloud users. Communications between apps and the KVS are arbitrated by “syncdefaultsd” and other

iCloud system services. The KVS is tied to each user's account and accessing it requires the targeted account's credentials or intercepted iCloud authentication tokens.

The vulnerability found by Radocea is related to Apple's open source implementation of the Off-The-Record (**OTR**) messaging protocol. Devices can only transmit OTR data if they are part of a group of trust called "signed syncing circle," which is signed with a syncing identity key associated with each device and a key derived from the user's iCloud password. Joining the circle requires permission from an existing device and user interaction. The researcher discovered that, due to improper error handling, the signature verification routine for OTR could have been bypassed, allowing an MitM attacker to negotiate an OTR session without needing the syncing identity key.

While an attacker cannot exploit this vulnerability to join a signing circle, it does allow them to impersonate other devices in the circle when keychain data is being synced, and intercept passwords and other secrets, the expert said.

Radocea has pointed out that it's often easy for attackers to **obtain iCloud passwords**, especially since many people set weak passwords or use the same one across multiple online services.
Apple said it addressed the vulnerability through improved validation for the authenticity of OTR packets.