Gravierende Sicherheitslücken in TwitterKit für iOS

Fraunhofer SIT warnt Entwickler: TwitterKit für iOS nicht mehr benutzen und austauschen

Das TwitterKit für iOS 3.4.2, das zahlreiche Apps zur Kommunikation mit Twitter nutzen, hat gravierende Sicherheitslücken, die Identitätsdiebstahl, Account-Missbrauch sowie Datenverluste zur Folge haben können. Das haben Sicherheitsforscher des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt herausgefunden. Es handelt sich um eine End-of-life-Softwarebibliothek von Twitter, die nicht mehr aktualisiert wird, aber noch in Apps zum Einsatz kommt. App-Entwickler sind dringend dazu aufgerufen, den TwitterKit für iOS-App-Entwicklungen nicht mehr einzusetzen und in bestehenden Apps durch Alternativen zu ersetzen. Technische Details zur gefundenen Sicherheitslücke finden sich hier: www.sit.fraunhofer.de/cve.

Die Softwarebibliothek TwitterKit für iOS 3.4.2 sowie dessen ältere Versionen werden in einigen beliebten Apps genutzt. Experten des Fraunhofer SIT haben einen Fehler in der Schnittstelle zu Twitter entdeckt, die das Twitter-SSL-Zertifikat nicht korrekt überprüft. Dadurch können Angreifer über eine man-in-the-middle-Attacke private Daten wie geschützte Tweets und Direktnachrichten des Twitternutzer-Accounts einsehen oder im Namen des Nutzers twittern, Tweets liken und retweeten. Darüber hinaus kann jede App angegriffen werden, die das schadhafte TwitterKit dafür nutzt, einen Login via Twitter anzubieten.

Die Sicherheitsforscher des Fraunhofer SIT haben Deutschlands beliebteste 2000 iOS-Apps gescannt (laut App Store) und 45 betroffene Apps gefunden. Von den mehr als zwei Millionen Apps in Apples App Store sind demnach vermutlich viele Anwendungen unterschiedlichster Kategorien betroffen. Darüber hinaus ist der TwitterKit für iOS auch in anderen Entwickler-Frameworks eingebunden, wie Google Fabric. Apps, die mit Google Fabric geschrieben worden sind, können somit auch von der Sicherheitslücke betroffen sein. Mehr technische Details zur Schwachstelle finden sich hier: www.sit.fraunhofer.de/cve.

Twitter stellt keinen Patch zur Verfügung

Die Fraunhofer-Experten haben Twitter unmittelbar vertraulich informiert. Daraufhin teilte Twitter mit, dass eine Schließung der Sicherheitslücke durch einen Patch nicht erfolgen wird, da der Support für den TwitterKit bereits Ende Oktober 2018 ausgelaufen ist. Die Twitter-eigene App Periscope ist jedoch mittlerweile gepatcht. Die Fraunhofer-Sicherheitsforscher wenden sich deshalb an alle App-Entwickler: „Wir wollen alle iOS-Entwickler dringend davor warnen, diese Softwarebibliothek zu nutzen oder im eigenen Code zu belassen. Das komplette TwitterKit ist unsicher“, sagt Dr. Jens Heider, Mobile-Security-Experte am Fraunhofer SIT. Twitter selbst nennt Alternativen zum hauseigenen TwitterKit unter folgendem Link: https://blog.twitter.com/developer/en_us/topics/tools/2018/discontinuing-support-for-twitter-kit-sdk.html

Nutzer: Login mit Twitter nicht verwenden

Ob und wie Smartphonenutzer selbst betroffen sind, lässt sich nicht ohne Weiteres feststellen. iOS-App-Nutzern rät Jens Heider deshalb, einen Login mit Twitter, der in einer App angeboten wird, nicht zu nutzen, insbesondere nicht, wenn die Smartphonenutzer sich in einem öffentlichen WLAN befinden. Hier lassen sich die Schwachstellen besonders leicht ausnutzen.

Die Sicherheitsexperten des Fraunhofer SIT haben die Schwachstelle im TwitterKit mithilfe des selbst entwickelten Testwerkzeugs Appicaptor gefunden. Auf der Security-Messe it-sa in Nürnberg vom 8.

bis 10. Oktober stellt das Fraunhofer SIT-Team die Erkenntnisse und das Tool vor, das große Mengen Apps automatisiert auf Sicherheitslücken hin scannen kann. Mehr Informationen zum Messeauftritt des Fraunhofer SIT finden sich unter www.sit.fraunhofer.de/itsa2019.