Millionen von Android- und Apple-Nutzern von Sicherheitslücke “FREAK” betroffen

Eine HTTPS-Sicherheitslücke, die seit langem besteht, wurde kürzlich entdeckt. Ihr Name: FREAK, das steht für “Factoring RSA Export Keys”. FREAK ist ein Produkt der 90er Jahre, als US-Politik den Einsatz starker Verschlüsselung verbot. Mehrere Websites sind davon davon betroffen, darunter Seiten von Regierungen und Kreditkartenunternehmen. Zu den potenziell betroffenen Plattformen zählen Geräte mit Android und iOS. Apple und Google haben beide Sicherheitspatches angekündigt, aber Art und Ausmaß dieser Sicherheitslücke sind besorgniserregend.

mehr unter: http://blog.emsisoft.com/de/2015/03/04/millionen-von-android-und-apple-nutzern-von-sicherheitslucke-freak-betroffen/#sthash.cdvBlyt0.dpuf