Scris de newsreporter pe 26 septembrie 2020, 15:28

Cum au spart hackerii WhatsApp cu un simplu apel telefonic

Un raport recent sustine ca renumita firma israeliana de spionaj NSO Group a dezvoltat un hack pentru WhatsApp care ar putea injecta malware pe telefoanele vizate – si le poate fura date – printr-un simplu apel telefonic, scrie Playtech.ro.

whatsapp-hack-1170x658.jpg

Tintele nici macar nu trebuie sa raspunda la apel pentru a fi hackuite, iar apelurile nu lasa urme in jurnalul telefonului.

A fost exploatata o vulnerabilitate a WhatsApp

WhatsApp, care ofera mesaje criptate in mod implicit pentru 1,5 miliarde de utilizatori din intreaga lume, a descoperit vulnerabilitatea la inceputul lunii mai si a lansat un patch.

Compania detinuta de Facebook a declarat ca a contactat o serie de grupuri pentru drepturile omului cu privire la aceasta problema si ca exploatarea acestei vulnerabilitati poarta “toate semnele distinctive ale unei companii private cunoscute ca lucreaza cu guvernele pentru a livra programe spion”.

intr-o declaratie, NSO Group a negat orice implicare in selectarea sau vizarea victimelor, dar nu si rolul sau in crearea hack-ului in sine. Asa-numitele bug-uri zero-day, in care atacatorii gasesc o vulnerabilitate inainte de a fi remediata de companie, sunt pe fiecare platforma.

Cu toate acestea, un hack care nu necesita altceva decat un apel telefonic pare o provocare unica – daca nu imposibil – de aparat.

> “Bug-uri exploatabile la distanta pot exista in orice aplicatie care primeste date din surse necredibile”, spune Karsten Nohl, inginer la firma germana Research Research Labs.

Aceasta include apelurile WhatsApp, careutilizeaza protocolul voice-over-internet (VoIP) pentru a conecta utilizatorii. Aplicatiile VoIP trebuie sa confirme apelurile primite si sa te anunte despre apel, chiar daca nu vrei sa-l preiei.

> “in cazul WhatsApp, protocolul pentru stabilirea unei conexiuni este destul de complex, deci exista cu siguranta loc pentru erori exploatabile care pot fi declansate fara ca persoana de la celalalt capat sa preia apelul”.

Nohl subliniaza ca lucrurile devin si mai complicate atunci cand apeluri sunt criptate end-to-end, asa cum face WhatsApp.

in timp ce WhatsApp isi bazeaza criptarea end-to-end pe Signal Protocol, apelurile sale VoIP includ probabil si alte coduri. Signal spune ca serviciul sau nu este vulnerabil la acest atac de apelare.

Ce a presupus aceasta exploatare

Conform recomandarilor de securitate ale Facebook,vulnerabilitatea WhatsApp provine dintr-un tip extrem de comun de bug cunoscut sub numele deoverflow buffer.

Aplicatiile au un buffer pentru a stoca date. O clasa populara de atacuri supraincarca strategic aceste buffere, astfel incat datele “se revarsa” in alte parti ale memoriei. Acest lucru poate provoca blocari sau, in unele cazuri, poate oferi atacatorilor un punct de sprijin pentru a castiga din ce in ce mai mult control.

Acest lucru s-a intamplat cu WhatsApp. Hack-ul exploateaza faptul ca, intr-un apel VoIP, sistemul trebuie pregatit pentru o serie de intrari posibile de la utilizator: preluati, refuzati apelul si asa mai departe.

> “Acest lucru suna intr-adevar ca un incident ciudat, dar in centrul acestuia pare sa existe o problema de depasire a bufferului, care, din pacate, nu este deloc neobisnuita in zilele noastre. Securitatea nu a fost niciodata obiectivul principal de proiectare al WhatsApp, ceea ce inseamna ca WhatsApp trebuie sa se bazeze pe stive complexe de VoIP cunoscute pentru vulnerabilitati.”
> Bjoern Rupp, CEO al companiei germane de comunicatii securizate CryptoPhone

Bug-ul WhatsApp a fost exploatat pentru a viza doar un numar mic de activisti si disidenti politici, astfel incat majoritatea oamenilor nu vor fi afectati cu nimic, in teorie. Dar ar trebui sa descarcati in continuare patch-ul pe dispozitivele dvs. Android si iOS.

Playtech.ro

ADRESA: http://crct.ro/nwIH