WhatsApp Vulnerable to Snooping

Introduction

On 13th January 2017, Guardian newspaper reported that WhatsApp, a mobile messaging service application owned by Facebook, is prone to interception due to vulnerability with its encryption method. This security flaw grant Facebook and others (middleman) to intercept and read encrypted messages easily.

Why is it important?

This attack can allow attacker to gain permission to access its server and reset the current encryption key but inserting the hacker’s own to push himself as a relay point [2]. This move would effectively intercept messages sent between parties ranging from 2 users to 256 members from a group chat. Facebook was already informed and aware of this vulnerability since April 2016 and its not working on a solution to resolve this issue.

Who is affected?

Users around the world would be deem vulnerable. As of 2017, there are more than a billion plus user login into this application as their messaging service. [3]

What impact might it have on people?

With more than a billion users, and with the convenience of the services provided by the application. Attackers might be able to intercept communication between the parties and serve as a middleman being read. Being able to reset the encryption key results to hackers invading the confidentiality of the system and data, which is currently authorized to Facebook only. This would also result to personal data being mined being threaten to more security issues like Ransomware. [4]

What were the causes?

The cause of this issue is due to the vulnerability where there is a weakness in the application server encryption system due to a security backdoor that Facebook implemented in its encryption protocol. Currently, the system is dependent on the encryption keys that are traded by users between one another which aids in securing their communication. However, the application itself can force generate these secure keys without the knowledge of the offline users.

Reference

[1] <https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages>

[2] http://www.theverge.com/2017/1/13/14266632/whatsapps-backdoor-vulnerability-key-reset-signal

[3]http://tech.firstpost.com/news-analysis/whatsapp-bumps-up-group-member-limit-from-100-to-256-is-it-time-for-spam-yet-297992.html

[4] http://www.straitstimes.com/world/europe/whatsapp-vulnerable-to-snooping-report