Detecting WhatsApp flaws allows an attacker to access files on the machine

This is a Cross-Site Scripting (XSS) vulnerability.

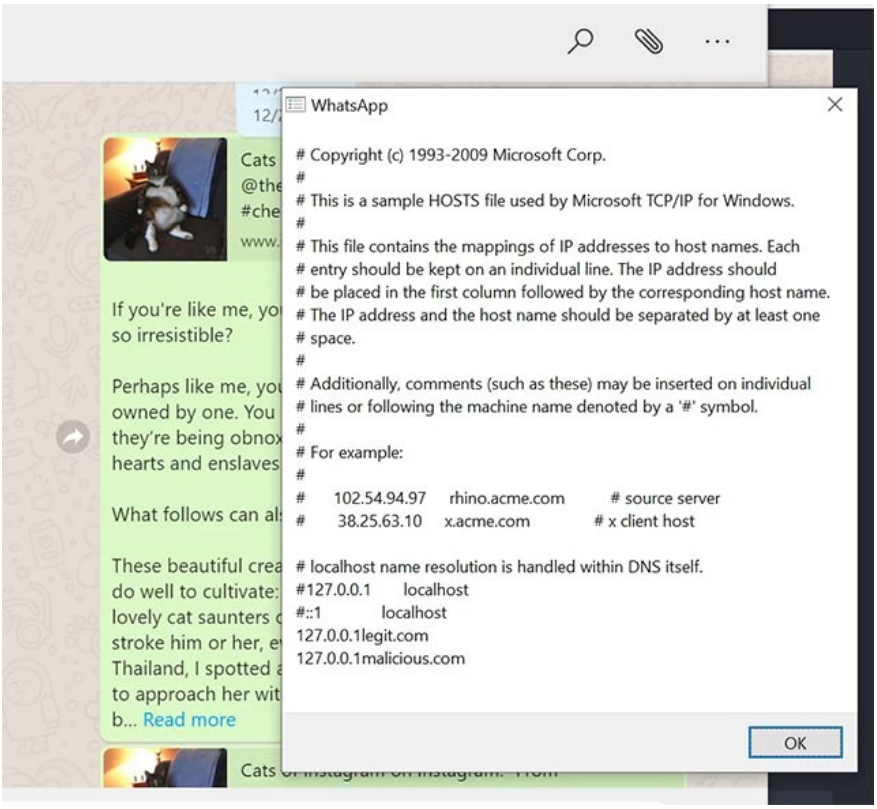
A group of international security researchers recently discovered and reported a critical vulnerability exists in the WhatsApp application, which could allow potential attackers to access the local file system of users, on both macOS and Windows platforms.

Specifically, this is a Cross-Site Scripting (XSS) vulnerability that exists in the process of pairing between the WhatsApp desktop application (WhatsApp Desktop) and the WhatsApp app for iPhone. If successfully exploited, it will allow hackers to access the device's local file system.

All versions of WhatsApp Desktop prior to v0.3.9309 were affected by this problem when setting up the pairing process with WhatsApp versions for iPhone from 2.20.10.

This vulnerability was tracked with the identifier CVE-2019-18426, and the severity was quite high (8.2). This is because it can be exploited remotely, but CVE-2019-18426 also requires user interaction to be successful.

The flaw was discovered by researcher Perimx Gal Weizman when he found an anomaly in WhatsApp's Content Security Policy (CSP), allowing malicious insertion through scripts to execute them on the client side - A typical form of XSS attack. The attack mechanism is described as follows.



The flaw appears on the Windows and Mac versions of the application, in the process of managing banners or previewing web links in messages. JavaScript that is embedded in a malicious banner can bypass victim protection and local file system access. According to the researchers, the heart of the flaw lies in the Chromium browser tool of the Electron application framework. WhatsApp relies on this framework to provide a user interface for its desktop clients. The hacker can then invade through the notification message appears completely normal, when the victim clicks on preview of the attached link from a message created by the hacker.

There have been no reports regarding the actual exploitation of the flaw, and Facebook has also released the corresponding patch. However, users are also advised to update their applications to the latest version to minimize any potential risks.