Thousands of iOS apps could be at risk because of an open source vulnerability

A vulnerability in open source software Cocoapods can put applications such as Facebook, TikTok, Netflix on iOS and macOS at risk of attack.

The research team of EVA Information Security, a cybersecurity and testing company in Israel, discovered a vulnerability in open source software Cocoapods that could put applications such as Facebook, TikTok, Netflix on iOS and macOS at risk of being attacked. labour.

Cocoapods is a widely used dependency manager for software projects coded in Swift and Objective-C programming languages.

Dependency Manager is an important tool in the software development process, allowing authentication and cryptographic signing of software packages.

Therefore, problems with Cocoapods will negatively affect many parts of the software or the web.

According to EVA Information Security, the vulnerability is the result of an uneven Cocoapods server migration process and may have existed since 2014, causing thousands of software library packages to no longer link to the original file and not origin can be traced.

This loophole allows attackers to replace the original source code with their own malicious code into the developer's software development tools. Because it went undetected for so long, it's possible that thousands of apps and millions of devices have been exposed over the years.

Hackers can take advantage of vulnerabilities to install ransomware or other types of malicious code into applications that have access to sensitive user information and collect them.

Also according to the research team, most iOS and macOS applications are coded in Swift and Objective-C languages, including popular names such as TikTok, Snapchat, LinkedIn, Netflix, Microsoft Teams, Facebook, Messenger . Therefore, the vulnerability in open source software Cocoapods could affect thousands of applications and "an attack on the mobile application ecosystem could infect most Apple devices, causing thousands of organizations to affected position.

According to the research team, Cocoapods has now patched the above errors. But the fact that they have gone undetected for nearly a decade is a cause for concern. The group recommends that developers review their product source code to determine whether the software is contaminated with errors.

Apple has not commented on this serious discovery.