XcodeGhost Advisory

xMatters Security Office

September 21, 2015

On Friday, September 18, 2015, security researchers from Palo Alto Networks announced that they had found compiler malware in Apple Xcode, the official Apple programming tool for iOS and OS X applications. They determined that this malware, known as XcodeGhost, had been introduced and uploaded to mirror sites hosted on the Baidu cloud sharing service used by many Chinese app developers and programmers.

The xMatters mobile app for the Apple iOS platform is not compromised by the XcodeGhost malware.

xMatters developers access Xcode only at the official Apple source, and development of the xMatters iOS platform is carried out only in North America. When the news of XcodeGhost was announced, the xMatters development teams checked their versions of Xcode and confirmed that the xMatters mobile app is not susceptible to XcodeGhost.

Resources:

- http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/
- http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/#
- http://www.bbc.com/news/technology-34311203