New security vulnerabilities on iOS 12.1 allow access to contacts and phone calls

A Youtuber named Jose Rodrigue discovered a serious security flaw of iOS 12.1 update, allowing to bypass the lock screen of all iPhones without the need for a password, face ID or fingerprint.

New iOS 12.1 update is released by Apple with many new features. However, only a few hours later, a Youtuber named Jose Rodrigue discovered a serious security error of this update, allowing to bypass the lock screen of all iPhones without needing a password, good face ID. fingerprints.

According to Jose Rodrigue, this vulnerability relates to the new Group Face Time feature Apple added in iOS 12.1 update. When the iPhone is in lock screen mode, Jose Rodrigue "takes advantage" of the virtual assistant Siri to make or receive calls. After that, the call is converted to Group Face Tim call, now you can access the menu on the bottom right and click the "Add Person" or "Add people" button to access the contacts and view the information. believe on iPhone.

However, Jose Rodrigue said it could temporarily prevent this vulnerability by accessing the iPhone Settings and turning off the option to order Siri on the lock screen.

This is not the first time, iOS 12 updates have a serious security error related to passing this lock screen. Previously, iOS 12.0.1 update also had errors that allowed it to bypass the lock screen and steal images stored in the device.

With previous updates of iOS 6.1, iOS 7 and iOS 8.1, there have been many similar errors.

See more:

1. iPhone X, iPhone 8 may slow down after upgrading to iOS 12.1
2. Three critical holes in Linksys routers, hackers can take advantage of hijacking