



Issued 10/18/18

New iOS Passcode Bypass Allows Viewing and Sharing Photos from Locked iPhones

Jose Rodriguez iOS enthusiast and hobbyist hacker managed to find a way to work around the iOS lock screen to view and share photos from a locked iPhone.

Rodriguez uploaded a video on YouTube showing how the vulnerability he found can be exploited with the help of accessibility features implemented by Apple within iOS to enable users with visual impairments to use their devices. Moreover, to be able to get around the iPhone's lock screen, one can use the VoiceOver feature and the Siri assistant to access the Photo Library, open photos and send them to another device chosen by the attacker. Apple just released iOS 12.0.1 on October 8 with fixes for two other passcode bypass bugs found by Rodriguez, and it seems that they will have to come up with another fix pretty soon to address this new security issue. The first CVE-2018-4380 bug also used the VoiceOver iOS Accessibility feature and allowed attackers with local access to iPhone 5s and later, iPad Air and later, and iPod touch 6th generation devices to view contacts and photos from the lock screen. The second bug patched in the iOS 12 release with the CVE-2018-4379 ID used the Quick Look feature to allow an attacker to preview and share documents stored on a locked iPhone 5s, and later, iPad Air and later, and iPod touch 6th generation device.