iOS 10 Passcode Bypass Can Access Photos, Contacts

By Chris Brook

Published: 2016-11-17 · Archived: 2026-04-05 17:59:25 UTC

A vulnerability in iOS 8, 9, 10, and even the most recent beta version, 10.2 beta 3, could allow an attacker to access photos and contacts on a locked iPhone.

A vulnerability in Apple's iOS versions 8, 9, and 10 could allow an attacker to access photos and contacts on a locked iPhone, according to two sources that posted videos showing how the password bypass works. According to both sources, the vulnerability also impacts the most recent version of iOS 10.2 beta 3.

The loophole involves tricking Siri and Apple's accessibility feature in iOS called VoiceOver to sidestep the device's passcode.

Owners of two different YouTube channels that specialize in Apple jailbreak news, tutorials, and reviews, iDeviceHelp and EverythingApplePro, disclosed the bug in videos posted this week.

Like most iPhone passcode bypasses, the process is a little far flung, but appears to work, provided the attacker has physical access to a device that has Siri enabled.

"It doesn't matter if you have [iOS' fingerprint recognition feature] Touch ID, a six code, or four code passcode, it works on all of them," Filip, who runs the channel EverythingApplePro says of the bypass, in his video.

To carry out the bypass, an attacker would also either need the phone number of the device or have to wait until someone calls it. In most instances, assuming a user has linked their phone number with their phone's 'contact' information, asking Siri "Who am I?" will display the number.

According to the two videos, a user could follow a series of seven steps to bypass the passcode:

Step 1: Call phone number of device.
Step 2: Device shows message icon – click 'Message' and then 'Custom' which takes you to the 'New Message' screen.
Step 3: Long press Siri button, say "Turn on Voice Over."
Step 4: Go back to the message screen, double tap bar where the caller's name is usually entered. Hold, immediately click the keyboard. Repeat until a slide-in effect on the iPhone's screen above the keyboard appears.
Step 5: Long press Siri to "Turn off VoiceOver," return to messages and type the first letter of a caller's name in top bar, tap (information) icon next to it, and create a new contact.
Step 6: Select 'add photo' and 'choose photo'. Attacker granted ability to view victim's photo gallery, despite the iPhone being in a locked state.
Step 7: Select a contact on the iPhone, granted ability to view previous conversations.

To fix the issue, at least in the short term, users can always disable Siri on their lock screen by going to Settings -> Touch ID & Passcode -> Disable Siri on the Lockscreen.

It's unclear when or if Apple will fix the issue, which reportedly also affects iPads. The company did not immediately return a request for comment on Thursday. Miguel Alvarado, who runs iDeviceHelp, suggested Wednesday however that Apple may fix the issue for 4S users in a future update, iOS 9.3.6:

iPhone passcode bypasses have become a common occurrence over the last few years and seem to pop up every couple of iOS releases. In March, researchers disclosed how an attacker could use Siri to bypass an iPhone's passcode to access native iOS apps like Clock and Event Calendar. That vulnerability affected iOS 9.0, 9.1 and 9.2.1.

Another bypass surfaced in April that affected iOS 9.3.1. That bypass could have allowed an attacker to bypass Siri to search Twitter and in turn gain access to photos and contacts on a device.
