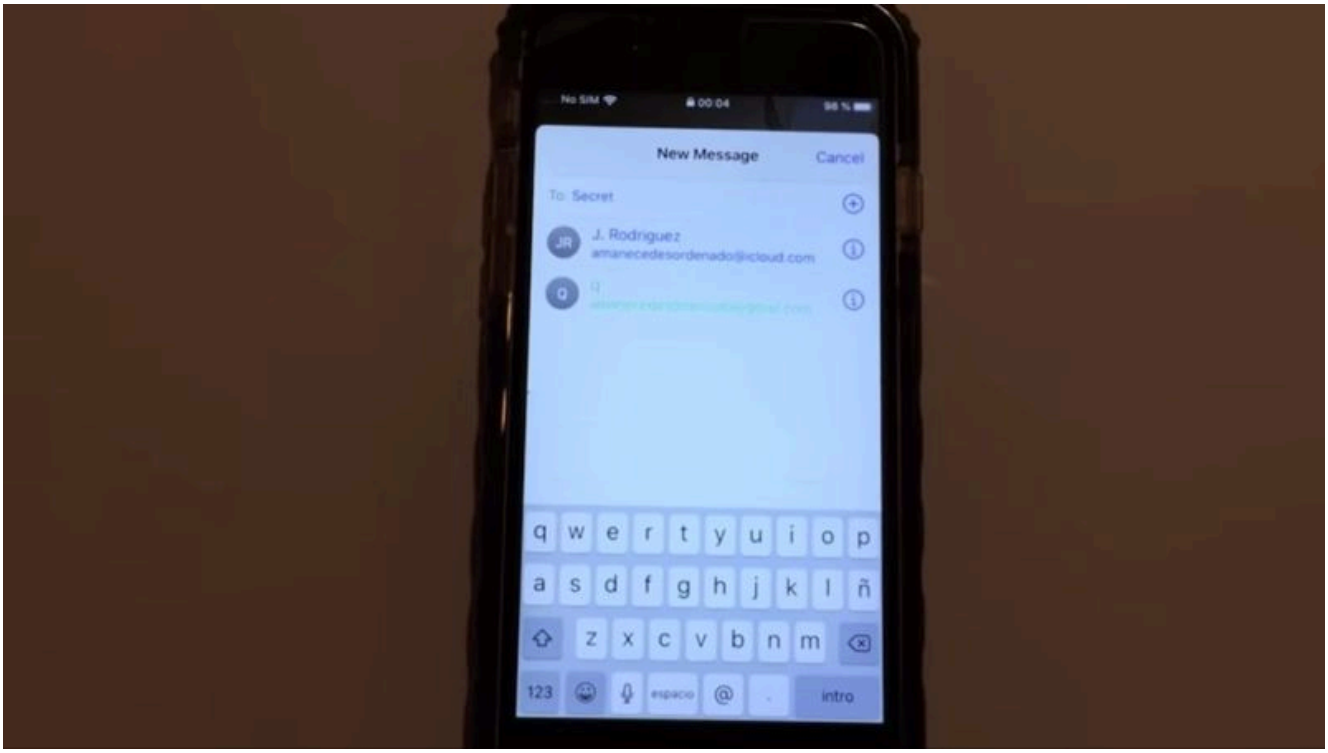
iOS 13 ships with known lockscreen bypass flaw that exposes contacts



Jose Rodriguez

reader comments

20 with 20 posters participating

Share this story

Apple released iOS 13 with a bunch of new features. But it also released the new OS with something else: a bug disclosed seven days ago that exposes contact details without requiring a passcode or biometric identification first.

Independent researcher Jose Rodriguez published a video demonstration of the flaw exactly one week ago. It can be exploited by receiving a FaceTime call and then using the voiceover feature from Siri to access the contact list. From

there, an unauthorized person could get names, phone numbers, email addresses, and any other information stored in the phone’s contacts list.

[embedded content]
Rodriquez’s video was the topic of more than 100 news articles over the past week. Since iOS 13 was in beta when it first appeared, I assumed Apple developers would fix the bypass in time for yesterday’s release. Alas, they didn’t, and it’s not clear why.

An Apple representative told Ars the bypass will be fixed in iOS 13.1, scheduled for release on Sept. 24.

As with all lockscreen bypasses, an exploit requires the attacker to have physical and uninterrupted access to a vulnerable phone. It can’t be exploited remotely by SMS or similar means. But the sole purpose of lockscreens is to protect against brief encounters by untrusted people. While the iPhone has suffered from much worse vulnerabilities—both the recent jailbreak bug regression and the host of actively exploited zeroday flaws come to mind—it’s hard to understand why this one wasn’t fixed before iOS went live.

It wouldn’t be surprising if Apple issued an update soon. Until then, users may be able to mitigate the threat by following instructions here.

Post updated to add comment from Apple.

https://arstechnica.com/?p=1572301