UNLOCKED —

Buffer overflow exploit can bypass Activation Lock on iPads running iOS 10.1.1

But the exploit relies on tricks that aren't possible on iPhones.

ANDREW CUNNINGHAM - 12/2/2016, 11:00 AM

Andrew Cunningham

Enlarge / The iPad Air 2 and Mini 4.

FURTHER READING
iOS 7 Activation Lock cutting iPhone theft, damaging resale market

Apple's Activation Lock feature, introduced in iOS 7 in 2013, deters thieves by associating your iPhone and iPad with your Apple ID. Even if a thief steals your device, puts it into Recovery Mode, and completely resets it, the phone or tablet won't work without the original user's Apple ID and password. This makes stolen iDevices less valuable since they become more difficult to resell, and it has significantly reduced iPhone theft in major cities.

The feature has been difficult to crack, but a new exploit disclosed by Vulnerability Lab security analyst

Benjamin Kunz Mejri uses a buffer overflow exploit and some iPad-specific bugs to bypass Activation Lock in iOS 10.1.1.

When you're setting up a freshly reset iPad with Activation Lock enabled, the first step is to hit "Choose Another Network" when you're asked to connect to Wi-Fi. Select a security type, and then input a very, very long string of characters into both the network name and network password fields (copying and pasting your increasingly long strings of characters can speed this up a bit). These fields were not intended to process overlong strings of characters, and the iPad will gradually slow down and then freeze as the strings become longer. During one of these freezes, rotate the tablet, close its Smart Cover for a moment, and then re-open the cover. The screen will glitch out for a moment before displaying the Home screen for a split second, at which point a well-timed press of the Home button can apparently bypass Activation Lock entirely (but it will have to be extremely well-timed, since the first-time setup screen will pop back up after a second).

This video shows the exploit in action, and we were able to reproduce it on an iPad Mini 2 running iOS 10.1.1. In our testing, however, we couldn't reproduce the bug on an iPhone 5 running iOS 10.1.1—the first-time setup screens on all iPhone models don't rotate as they do on the iPad, nor can the iPhones be locked with Smart Covers. These screens also wouldn't rotate into landscape mode in iPads running iOS 9, so if you haven't updated yet (or if you're using an older iPad and can't update), you're probably vulnerable to a whole bunch of other security bugs, but it's not possible to make the screen glitch out in the same way.

FURTHER READING
How security flaws work: The buffer overflow

There could be an alternate form of the exploit that works on iPhones, though as of this writing it only appears to be possible on iPads running iOS 10.1.1. We've contacted Apple for comment and will update if we receive a response.

ANDREW CUNNINGHAM
Andrew has a B.A. in Classics from Kenyon College and has over five years of experience in IT. His work has appeared on Charge Shot!!! and AnandTech, and he records a weekly book podcast called Overdue.

EMAIL andrew.cunningham@arstechnica.com // **TWITTER** @AndrewWrites

READER COMMENTS 53 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS