

Forum:[Hack Forums](#)

Thread: [Iphone 7/7 plus Recovery Mode Bruteforce Exploit](#)

?Criminal - August 18, 2017, 6:37 pm

Did anyone hear about this recently? apparently the pin prompt on this specific page is missing the phone self destruct after 10 tries check or the lockout policy allowing infinite tries, I'm not sure why it only works on the iphone 7 and 7 plus if anyone could explain that would be interesting to know.

TheWHO? - August 19, 2017, 11:11 am

Yeah check out this video buddy.

[Video: <https://www.youtube.com/watch?v=IXglwbyMydM&t=627s>]

Zexo - August 19, 2017, 11:19 am

Smh apple needs to fix this shit soon.

/wrists - August 19, 2017, 11:22 am

Yalu JB Wrote:A new Chinese \$500 box-like device can hack into your passcode automatically! This tool is based on a recovery mode security vulnerability that allows it to input an infinite amount of passcodes.

It looks very primitive at the very outset but packs incredible power for such a small device. It comes with 3 USB slots, which allows the hacker to hack 3 iPhone devices simultaneously.

Furthermore, it also has with its own hacking software that has a number of options pertaining to the cracking technique you want to use.

To initiate the hack, your device must be in the "flash" state, that is, must be undergoing the restore process.

The hacking methodology is very similar to a WiFi attack. It performs a classic brute-force attack and tries every combination of all the numbers until it gets it right.

Even if it does take time, it will still eventually cracking up the passcode since it can perform any number of attempts.

Will Apple close this loophole?

Yes, of course. Apple will be closing this major loophole as soon as possible now that this tool is public. As far as I know, it has already been closed in iOS 11.

With that said, you do not have to wait for them to fix every loophole or vulnerability. You can simply use several basic security functions already at your disposal to stay safe.

hacker

The best way to secure your device is to use an alphabetic password. Doing so will practically render all brute-force tools useless because they will then need to go through a humongous amount of combinations that could take up years.

That's all I could pull up.

iPhoo - August 20, 2017, 9:58 pm

(Aug 19, 2017 11:11 AM)Arnold Schwarzenegger Wrote: [\[CITE\]](#) Yeah check out this video buddy. youtube.com/watch?v=IXglwbyMydM&t=627s

Okay, but let's be smart. In theory the box is not needed at all. This is pretty much a rip-off. I've seen this recover data screen, while updating.

Now, more to the point: as long as you have a USB to lightning adapter, and a USB keyboard, you can make the PIN attempts yourself, or use a USB HID emulator. Which is not hard to make. With the emulator, you can script it to make pin attempts within set ranges.

Even manual entry is possible right? Although that would take forever. You can use logic to try common pins first (2580, 3669, 1245, 0852...) ?

?Criminal - August 20, 2017, 11:00 pm

(Aug 20, 2017 09:58 PM)iPhoo Wrote: [\[CITE\]](#) Okay, but let's be smart. In theory the box is not needed at all. This is pretty much a rip-off. I've seen this recover data screen, while updating.

Now, more to the point: as long as you have a USB to lightning adapter, and a USB keyboard, you can make the PIN attempts yourself, or use a USB HID emulator. Which is not hard to make. With the emulator, you can script it to make pin attempts within set ranges.

Even manual entry is possible right? Although that would take forever. You can use logic to try common pins first (2580, 3669, 1245, 0852...) ?

What im curious about is why this only works on the iphone 7 is there certain hardware that the iphone 7 has that causes this bug or can you not access this recovery page on iphones before the 7 like 6s 6 5s etc I figure since it's a software bug in the IOS update process it should in theory work on all devices unless recovery mode is like a special OS seperate from the main OS kinda like what self encrypted HDD's do you get booted into a special OS before the main one launches.

iPhoo - September 2, 2017, 12:31 pm

(Aug 20, 2017 11:00 PM)?Criminal Wrote: [\[CITE\]](#) What im curious about is why this only works on the iphone 7 is there certain hardware that the iphone 7 has that causes this bug or can you not access this recovery page on iphones before the 7 like 6s 6 5s etc I figure since it's a software bug in the IOS update process it should in theory work on all devices unless recovery mode is like a special OS seperate from the main OS kinda like what self encrypted HDD's do you get booted into a special OS before the main one launches.

I'm curious as well, I think it's a combination of hardware and software and maybe the lightning port on iPhone 7 and 7 plus is different. Although the only reason why it would have changed is because it now carries audio as well, since no headphone jack.

Still, maybe a custom firmware can be loading to reproduce the issues, but Apple doesn't sign custom firmware so that would be impossible I think?

Has no one tried to test my theory yet? I got a USB lightning adapter yesterday so maybe I will try loading the beta firmware, downgrading to 10.3.3 to get to the data recovery screen in the video and see if a USB keyboard will provide readable input.

What concerns me is it won't work, and there's some special exploit that they discovered and loaded into the IP box itself.... which would explain the high price. However it can probably be reverse engineered, but time is of the essence as these firmwares will no be longer be signed by Apple starting a couple weeks.

Really would like some help figuring it out.

Specifically, I'm stuck because my free Apple Dev account only qualifies for Xcode downloads?

imgur.com/a/XcGyd

Is there an unofficial mirror for iOS 11 beta downloads? I'm googling now but not seeing anything, which is really surprising but I wouldn't doubt Apple asks google to remove what they consider infringing links.

EDIT: SOLVED. Found this

reddit.com/r/iOSBeta/comments/6x8boo/download_official_apple_ios_11_developer_beta_9/

I hope this experiment works.

iPhoo - December 11, 2017, 3:32 pm

Wanted to report back, I remember trying this but the phone wouldn't boot up after restoring the firmware, and upgrading it.