Checkm8 iPhone exploit becomes talk of jailbreak town

September 29 2019, by Nancy Cohen

Credit: CC0 Public Domain

An unpatchable exploit in iOS devices could lead to a permanent jailbreak in generations of phones. Dan Goodin in *Ars Technica* put the number at 11 generations of iPhones, from the 4S to the X.

He was reporting on the security researcher who had revealed that a permanent unpatchable bootrom exploit might lead to permanent jailbreak of Apple iPhone 4S to iPhone X. ("Because the bootrom is contained in read-only memory inside a chip," said Goodin, "jailbreak vulnerabilities that reside there can't be patched.")

On Twitter, axi0nX, a security researcher, shared the Apple iOS jailbreak tool called checkm8. As noted in *International Business Times*, many tech watchers regarded this as epic.

The exploit was described as "a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices." The code was released on GitHub. But just what was released is important to say.

Tom's Hardware: "The developer noted that what he's releasing today is not a full jailbreak, but only the exploit for the bootrom." It's an exploit that *could* lead to a jailbreak with further work. For them to strip Apple's control away from the device and do what ever they wanted on it, "some additional exploits would be required," said Thomas Brewster in *Forbes*.

The exploit discovery affects iPhone 4s all the way up to iPhone X. In addition, said Lucian Armasu, *Tom's Hardware*, iPads using chips from A5 to A11 were affected by the exploit.

The editor for *9to5Mac*, Michael Potuck, reported on how the discovery was made known. "Twitter user, axi0mX shared their iPhone exploit.

The hack has been dubbed checkm8 by a researcher who goes by the name axi0mX.

"Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip)," according to the axi0mX tweet.

What kinds of damage can be done? Thomas Brewster, who covers security for *Forbes*, said "hackers can take the code released by axi0mX on GitHub and potentially load firmware (the core of the operating system) onto an iPhone."

Dan Goodin responded to that tweet: "The jailbreaking exploit released Friday prompted lots of security concerns. But it turns out it's not remotely exploitable, doesn't have persistence, and can't bypass the Secure Enclave."

Here is a fuller view of exploit limitations from *Ars Technica*: (1) Checkm8 requires physical access to the phone. It can't be remotely executed, even if combined with other exploits (2) the exploit allows only tethered jailbreaks (3) Checkm8 doesn't bypass the protections offered by the Secure Enclave and Touch ID.

All in all, said reports, anyone hoping to use checkm8 for abuse would be able to do only under very limited circumstances.

In his own words axi0mX discussed checkm8 in a Q&A with *Ars Technica*.

"A: This exploit works only in memory, so it doesn't have anything that persists after reboot. Once you reboot the phone... then your phone is back to an unexploited state. That doesn't mean that you can't do other things because you have full control of the device that would modify things. But the exploit itself does not actually perform any changes. It's all until you reboot the device."

Goodin asked if there was much chance someone was going to chain checkm8 to something else and get results with newer iPhones?

"A: I can't say it's impossible, and there are some really good hackers out

there. It's always possible. I think it's unlikely. I know I couldn't do it. The chance is always there, but I think it's very unlikely."

More information: github.com/axi0mX/ipwndfu

twitter.com/axi0mX/status/1177542201670168576?s=20

© 2019 Science X Network

Citation: Checkm8 iPhone exploit becomes talk of jailbreak town (2019, September 29) retrieved 23 April 2024 from https://techxplore.com/news/2019-09-checkm8-iphone-exploit-jailbreak-town.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.