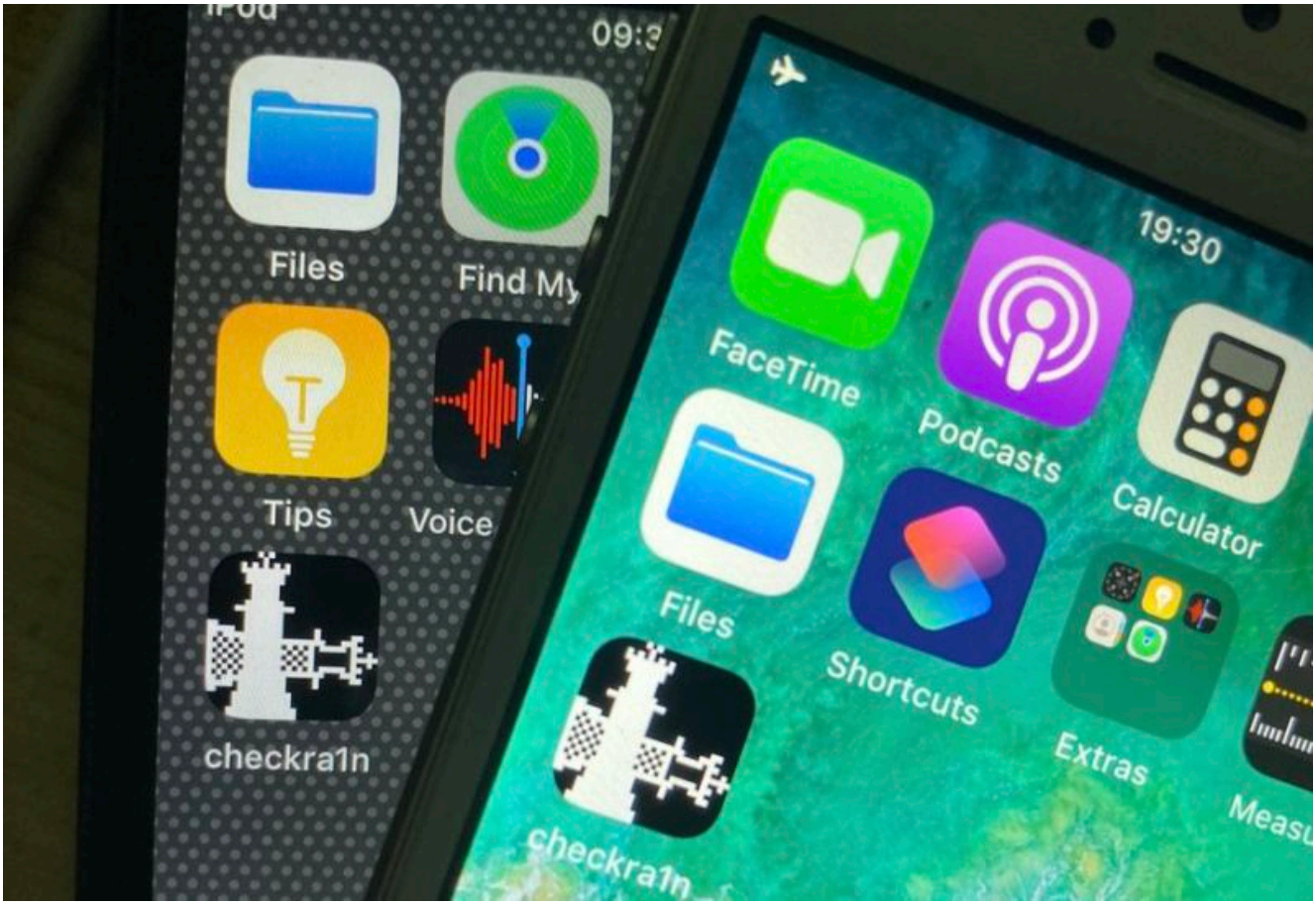
What the newly released Checkra1n jailbreak means for iDevice security



reader comments

55 with 41 posters participating

Share this story

It has been a week since the release of Checkra1n, the world's first jailbreak for devices running Apple's iOS 13. Because jailbreaks are so powerful and by definition disable a host of protections built into the OS, many people have rightly been eyeing Checkra1n—and the Checkm8 exploit it relies on—cautiously. What follows is a list of pros and cons for readers to ponder, with a particular emphasis on security.

The good

First, Checkra1n is extremely reliable and robust, particularly for a tool that's still in beta mode. It jailbreaks a variety of older iDevices quickly and reliably. It also installs an SSH server and other utilities, a bonus that makes the tool ideal for researchers and hobbyists who want to dig into the internals of their devices.

"I expected it to be a little rougher around the edges for the first release," Ryan Stortz, an iOS security expert and principal security researcher at the firm Trail of Bits, said in an interview. "It's really nice to be able to install a new developer beta on your development iPhone and have all your tooling work out of the box. It makes testing Apple's updates much much easier."

Another benefit of Checkra1n is that it promises to work reliably on a wide array of hardware. Those models include devices from the iPhone 5s all the way to the iPhone X running iOS 12.3 or later. (At the moment, the Checkra1n beta doesn't support the iPad Air 2, first generation iPad Pro, and fifth generation iPad. Users may also experience problems when running this beta on the iPhone 5s, iPad mini 2, and iPad mini 3. These incompatibilities will likely be fixed in time, as new Checkra1n updates become available.)

Also significant, Checkm8-based jailbreaks will work permanently on these devices. Unlike most jailbreaks, which exploit vulnerabilities in iOS, Checkm8 targets a flaw in the Boot ROM, which is the first code that runs when an iDevice is turned on. This code is burned into the hardware itself and can't be patched. This is the reason Checkra1n will work with every new release of iOS over the lifetime of a vulnerable phone.

This means that people can continue to enjoy the benefits and security fixes available in new iOS releases without losing

the ability to jailbreak their devices (new versions of iOS inevitably fix jailbreaking vulnerabilities). This is a far cry from jailbreaks over the past decade that forced users to run outdated versions of iOS. The last time a jailbreak targeted the Boot ROM was in 2010 when hacker George Hotz (aka Geohot) developed one for the iPhone 3GS and iPhone 4.

Checkra1n is also helpful because it makes it painfully obvious it has been used. A large Checkra1n logo displays during bootup. And the home screen will include the Cydia and Checkra1n apps, neither of which appear when an iDevice runs normally.

And like all Checkm8-based jailbreaks, Checkra1n requires physical access to the vulnerable device and a reboot, which means user data and Touch ID and Face ID are inaccessible until the next time a PIN is entered to unlock the device. This means that remote exploits aren’t possible.

The bad

Checkm8-based jailbreaks, including Checkra1n, come with some notable limitations that many jailbreaking enthusiasts consider deal-breakers. First, Checkm8 doesn’t work on iDevices introduced in the past two years, specifically those with A12 and A13 CPUs. That limits the jailbreak to older devices, most of which—but not all—are no longer sold in retail outlets.

The other major limitation is that Checkm8-based jailbreaks are “tethered,” meaning they don’t survive a reboot. Each time the device is restarted, it must first be connected to a Mac—eventually Windows versions of Checkra1n are expected—and jailbroken all over again. Untethered jailbreaks, by contrast, are much more popular because they allow iDevices to boot normally, without being connected to a computer each time.

Another drawback to any jailbreak is that it’s an inevitably

risky thing, since it unbinds an iDevice from the protections and quality assurances Apple has painstakingly built into iOS over more than a decade. Apple warns here that jailbreaking can "cause security vulnerabilities, instability, shortened battery life, and other issues." The stakes are raised further by the beta status of Checkra1n. The Checkra1n website warns: "This release is an early beta preview and as such should not be installed on a primary device. We strongly recommend proceeding with caution."

Then there are the risks of error by inexperienced users who are drawn to Checkra1n's reliability, robustness, and its promise to work—on older devices, anyway—in perpetuity.

"The biggest threat from Checkra1n is how easily a non-technical user can jailbreak their device, which then leaves it vulnerable to additional attacks," Christoph Hebeisen, head of security research at mobile security provider Lookout, said. One protection that Checkra1n deactivates is the iOS sandbox, which cordons off sensitive parts of iOS from the apps it runs. The risk is heightened by the ability of jailbroken devices to run any app. Normally iPhones and iPads can run only apps that are available in the App Store, which vets submissions for security and stability before allowing them in.

One other warning: the site checkrain[.]com is an imposter site that installs a malicious profile onto the end-user device. Readers should steer clear.

The (more subtly) bad

There's a more subtle threat posed by Checkra1n's ease in almost completely unpairing a device from the protections that have made iOS arguably the world's most secure OS. As noted earlier, it would be hard for someone to use this jailbreak maliciously against someone else. But Stortz, the iOS security expert at Trail of Bits, said that Checkra1n's release

demonstrates just how powerful it could be should its capabilities fall into the wrong hands.

“The threat is more real now because a sophisticated exploit is available to everyone,” he said. He went on to theorize cases of attackers reverse-engineering Checkra1n and combining its jailbreaking capabilities with rootkits or other malicious code. All attackers might need to use this malicious Checkra1n-derived jailbreak is very brief access to an iDevice. This type of attack could covertly steal text messages, login credentials, cryptographic keys, and all kinds of other sensitive data. These attacks would be particularly effective against iPhones and iPads that don’t use fingerprints or face scans for unlocking. He explained:

> *Checkm8 allows someone to undermine the trust of the iOS secure boot chain. Checkra1n makes it easy to do. It’s true that checkra1n puts a nice logo on it and installs development tools, but that doesn’t need to happen. Someone will modify checkra1n to remove the logo and install a rootkit instead. [In that scenario] having a PIN-only passcode is a poor choice. You’ll pick up your phone [after Checkra1n is surreptitiously installed] and unlock it, allowing the rootkit full access to your personal data.*

It has been possible to create this type of malicious jailbreak since late September, when the Checkm8 exploit became public. But that kind of attack required huge amounts of time and skill. Now, Stortz said, “no one would do that when Checkra1n exists and is so well done.”

The take-away from the sort of scenario Stortz hypothesizes is this: for journalists, dissidents, and other high-value targets who use iOS devices and can afford to, it’s best to use hardware that has an A12 or higher CPU. An iDevice introduced in the past two years will ensure that it’s safe from Checkra1n-derived attacks at border crossings, in hotel

rooms, or in other situations that involve brief separations.

For iOS users who can’t afford a newer iPhone or iPad, using Touch ID or Face ID can lower the chances of malicious jailbreaks since users can be tipped off that something is amiss if the iDevice unexpectedly requires a PIN. And whenever the device has been out of the user’s control, even briefly—or users suspect anything else is amiss—they should reboot it.

This level of scrutiny is probably overkill for most users of vulnerable iPhones and iPads. Unfortunately, for users belonging to more targeted groups, these precautions are a natural consequence of a post-Checkra1n era.

https://arstechnica.com/?p=1602451