Apple iPhones could have been hacked for years – here's what to do about it

September 5 2019, by Leslie Sikos And Paul Haskell-Dowland

Credit: CC0 Public Domain

For many years, the Apple iPhone has been considered one of the most secure smart phones available. But despite this reputation, security issues that might affect millions of users came to light last week, when

researchers at Google revealed they had discovered websites that can infect iPhones, iPads, and iPods with dangerous software.

Simply visiting one of these websites is enough to infect your device with malicious software, allowing a high level of access to the device. Worryingly, it seems these vulnerabilities have been "in the wild" (that is, actively used by cyber-criminals) for around two years.

As there is no visible sign of infection on the device, it is likely users are completely unaware of the risks they're facing.

The vulnerabilities being exploited are present on devices running recent (but not the most recent) versions of Apple's iOS operating system—specifically, iOS 10 through to early versions of iOS 12. Every device running the vulnerable versions of iOS is a potential target for these websites.

Devices are infected via several methods, using 14 different security flaws—an unusual number of ways to compromise a device. Worse is that seven of the flaws involve Safari, the default web browser for many of these devices (and web browsing is a common activity for many users).

It's not all bad news though. After Google reported the issues to Apple earlier this year, the vulnerabilities were promptly patched with the latest release of iOS (12.4.1).

Any user updating their device to the latest version of iOS should be protected against this attack. The easiest way to do it is to go to Settings > General > Software Update on your phone and then follow the prompts.

What happens when you visit an infected site?

As soon you open the web page, malicious software is installed on the device. This software has the potential to access location data and information stored by various apps (such as iMessage, WhatsApp, and Google Hangouts).

This information can be transmitted to a remote location and potentially misused by an attacker. The information extracted can include messages that are otherwise protected when sent and received by the user, removing the protection offered through encryption. Hackers can also potentially access private files stored on the device, including photos, emails, contact lists, and sensitive information such as WiFi passwords.

All of this data has value and can be sold on the Internet to other cyber-criminals.

According to antivirus firm Malwarebytes, the malicious software is removed when the infected device is restarted. While this limits the amount of time that the device is compromised, the user risks being reinfected the next time they visit the same website (if still using a vulnerable version of iOS).

The list of websites involved has not yet been made publicly available, so users have no means to protect themselves other than by updating their device's operating system. But we do know the number of visitors to these sites are estimated in the thousands per week.

Are Apple devices no longer secure?

High-profile attacks on these devices might dispel the myth that Apple devices are not susceptible to serious security breaches. However, Apple does have a bug-bounty program that offers a US$1 million reward to users who report problems that help to identify security flaws.

But considering the impact of this incident, it's obvious someone out there is making considerable efforts to target Apple devices. While the tech giant regularly updates its software, there have been recent incidents in which previously fixed security flaws were reintroduced. This highlights the complexity of these devices and the challenge of maintaining a secure platform.

The most important lesson for Apple's millions of users is to ensure you keep up to date with the latest patches and fixes. Simply installing the latest iOS update is sufficient to remove the threats caused by this vulnerability.

If you're concerned your details may have been stolen, changing passwords and checking your credit card and bank account statements are also important steps to take.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation