How iPhone vulnerabilities allow websites to hack iOS devices

How can websites hack iPhone? And what should you do to keep yourself safe from hacks like this? The following article will have all the details you need to know.

You may have heard about the discovery of a hack targeting iPhone devices through websites for years. Google claims it has discovered the issue as part of Project Zero's security analysis mission and shows hackers may have accessed thousands of devices over a two-year period.

So how can websites hack iPhones? And what should you do to keep yourself safe from hacks like this? The following article will have all the details you need to know.

Hacking iOS devices via websites - It's possible

1. How can websites hack iPhone?
2. What are the consequences of these hacks?
3. Who do these hacks affect?
4. What should iPhone users do about avoiding hacks?

How can websites hack iPhone?

Here's how this security issue affects iPhone devices, revealed in August 2019 by Google Project Zero. Traditionally, people thought it was difficult or even impossible to hack iOS devices as long as they were not jailbroken. To hack an iOS device requires zero day knowledge.

This is an undisclosed vulnerability to Apple or the security community. As soon as Apple discovered the security flaw, they fixed it. This means that as soon as a flaw is known to a large extent, it will almost immediately be fixed.

However, in the case of these hacks, websites can hack iPhones that have accessed them. Hackers have achieved this by using 14 different vulnerabilities, combined into 5 attack chains.

The attack chain is where several vulnerabilities are used in combination with one another to attack a device. A single security flaw won't be enough to hack a device, but when put together, they can do it. Hackers can combine the use of security holes together to install a monitoring software, run as the root on the device.

That means it defeats the operating system's security protocols and gains the highest possible security privileges.

Just visiting one of these sites is enough for your device to have surveillance software installed. More worrying, Google says it estimates that thousands of people visit these sites every week. This means that hackers have likely infected thousands of devices in the past few years.

What are the consequences of these hacks?

The list of privileges these hacks are really worrying about. Installed software can locate the device in real time, view call and SMS history, view notes in the Notes app, view passwords, listen to voice memos and view photos. The software can even see encrypted messages like those shared on multiple apps like iMessage, Telegram or WhatsApp.

Installed software can view encrypted messages because it has access to the database files on the phone. These files allow you to read and send encrypted messages. The operating system will protect these files from third-party applications. But because the software that was originally installed has root access, it can view these files and use them to read encrypted messages.

It can also upload emails from your phone to a hacker server, or you can copy all the contacts stored on your phone. Real-time GPS tracking is especially frightening because it means that hackers can see a user's current location anytime and track their movements.

Who do these hacks affect?

Apple has issued a statement addressing this issue. According to Apple, 'this sophisticated attack only affects a small extent, not a widespread exploit that affects all iPhone devices'. The company added, 'This attack affected about a dozen websites, focusing on content related to the Uighur community (Uighur in English).

Uighurs are an ethnic group of Chinese origin. The implication in Apple's statement is that the Chinese government may have used malware on iPhones to spy on Uighurs in particular, to monitor and control them.

Apple accuses Google of causing undue fear, causing all iPhone users to think their device has been compromised. This implies that most iPhone users need not worry about hacks, as they are aimed at only a small number of people. However, all users should be aware of the fact that these vulnerabilities exist and are used to harm iOS devices for two reasons.

Firstly, using these vulnerabilities to target a minority group is something everyone should be concerned about. Second, it proves that iOS devices can't be hacked and that iPhone users need to be aware of security issues.

Also, the potential dangers of this hack might be worth considering. Hackers only care about targeting certain groups of people. If desired, however, they could use the same method to infect iPhone devices on a much wider scale.

What should iPhone users do about avoiding hacks?

Although this news sounds scary, iPhone users don't need to panic. Apple has patched this vulnerability a while ago. As long as you're running iOS 12.1.4 or higher, you're currently 'immune' to this attack. This shows why updating device software regularly is so important. Companies often fix security issues like these in the latest version of software.

If you think your device has been infected with malware, you should update it to the latest version of iOS as soon as possible. The phone will reboot as part of the installation process. New software and rebooting will remove the malware from your device.

Unfortunately, it is not possible to run antivirus software on iOS. This means there's no way to test your device and detect threats, like this malware, in the future. The best thing you can do to keep your device safe is to update it regularly.

Although the iPhone is still a very secure device overall, it's not perfect. As demonstrated, it is possible to hack iOS devices and steal vast amounts of data from them.

To help keep your iPhone safe, you can learn about iPhone security apps and settings that you must know.

Good luck!