7 Apple hacks, breaches, and security vulnerabilities you didn't know about

Apple is no stranger to security incidents, be they a hack, breach or security vulnerability. You may not be aware of these different problems, and some may still put you at risk.

Apple is no stranger to security incidents, be they a hack, breach or security vulnerability. You may not be aware of these different problems, and some may still put you at risk. So what Apple hacks, breaches, and vulnerabilities do you need to know about?

Apple hacks and breaches

Apple has seen its fair share of hacks over the years, some of which have been particularly egregious. Let's start with a hack that took place more than a decade ago.

1. Hack XCodeGhost (2015)

In 2015, 128 million iPhone users were affected by a malware-based hack. Hackers used a malicious version of XCode, Apple's development environment for all of its operating systems, including iOS. With this malware, called XCodeGhost, hackers managed to compromise around 50 apps from the Apple App Store. People who downloaded the affected apps were vulnerable to hacking, and an estimated 500 million users were at risk at the time.

While this huge estimate is actually a bit smaller, documents provided during Apple's court battle with Epic Games revealed that 128 million individuals were still affected, including 18 million users in the United States (as reported by Security).

What's especially controversial about this incident is that at the time, Apple decided not to notify users who were at risk of being hacked. It took another 6 years for the public to become aware of the true nature of the hack, which came to light in the aforementioned legal trial between Apple and Epic Games.

2. Pegasus spyware (2016 onwards)

The infamous Pegasus spyware first launched in 2016 but rose to global prominence in 2021 when it was used to exploit iOS in highly targeted attacks. Pegasus was developed by Israel's NSO Group, a controversial organization that has made security news many times in the past. In fact, NSO Group sold its Pegasus spyware to many governments and states, including India and Mexico.

In this Apple exploit, an iOS vulnerability was abused to run Pegasus spyware on iPhones. An official statement from Apple explains that features like Lockdown Mode can be used to protect against such attacks, as can strong passwords and software updates. Threat notifications will be used to warn users who may have been targeted by state-sponsored hackers.

3. SolarWind (2021)

The SolarWinds attack rocked the technology and cybersecurity industry in 2021, and Apple couldn't avoid the wave.

In the SolarWinds attack, hackers exploited an iOS 14 zero-day vulnerability to infiltrate iPhones. Through this vulnerability, hackers used malicious domains to redirect iPhone users to phishing websites. This, in turn, allows attackers to steal user credentials, which can then be used to hack accounts or sell to other illegals on illegal marketplaces.

4. Apple and Meta data leak (2021)

Apple's most recent security incident took place in mid-2021 when Apple and Meta employees were scammed by hackers impersonating law enforcement officials. In the attack, hackers first infiltrated the accounts and networks of law enforcement agencies, then sent fake emergency data requests to employees of the two tech giants, asking for a response. recover quickly. In response to this seemingly official request, the user's IP address, home address, and contact number were provided.

It's important to note that Apple and Meta employees do not provide information due to random requests. Legitimate systems were hijacked by attackers to send requests, which made detection difficult.

Apple's vulnerabilities

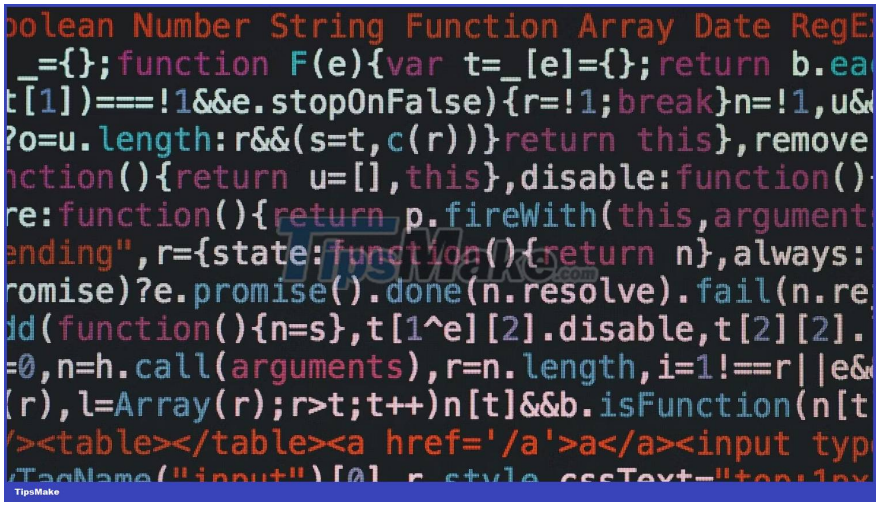
Apple's various software programs, including the operating system, can fall victim to code vulnerabilities.

1. Kernel and WebKit Vulnerabilities (2022)

In August 2022, Apple announced that it had found a kernel vulnerability (officially named CVE-2022-32894) that allows arbitrary code execution with kernel privileges. Apple has patched CVE-2022-32894 with macOS Monterey, so if you installed this update manually or are using a version of macOS newer than Monterey, there's no need to worry.

Along with this vulnerability, an Apple WebKit vulnerability was also discovered. This vulnerability also poses the risk of arbitrary code execution due to malicious web content. Like the above vulnerability, the WebKit vulnerability for macOS Monterey has been patched a long time ago.

2. Blastpass Vulnerability (2023)



In September 2023, two Apple zero-day vulnerabilities were discovered that were exploited by attackers. The vulnerabilities are officially named CVE-2023-41064 and CVE-2023-41061, in iOS software.

CVE-2023-41064 is a buffer overflow vulnerability that allows arbitrary code execution and may affect all iPhone model 8 and later running iOS 16.6 or later. Some iPad models can also be targeted through this vulnerability. CVE-2023-41061, discovered shortly after the first vulnerability, is an authentication issue that can be abused through malicious attachments.

According to a report by The Citizen Lab, when used together, these two vulnerabilities form an exploit chain called Blastpass and form part of NSO Group's Pegasus spyware distribution chain. Blastpass can be used to hack iPhones and iPads without the victim even needing to interact with any malicious website or communication. This is also known as a zero-click vulnerability.

However, by using Apple's Lockdown Mode, the chain can be stopped in its tracks, preventing it from infecting your device. There is also a patch for two currently exploited vulnerabilities.

3. Foundation Vulnerability (2023)

In early 2023, three Apple zero-day vulnerabilities were discovered that put many Apple operating systems at risk, including iOS, iPadOS, and macOS. Two of the vulnerabilities were found in Apple's Foundation framework, which provides a base level of functionality and interaction for Apple's apps. These three vulnerabilities, known as CVE-2023-23530, CVE-2023-23531, and CVE-2023-23520, provided attackers with the ability to remotely execute malicious code on infected devices.

In February 2023, Apple patched these three security vulnerabilities, so you will no longer be exposed to them if you update your Apple device regularly.

You finished reading the article "**7 Apple hacks, breaches, and security vulnerabilities you didn't know about**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.