Apple releases iOS 14.4.2, iOS 12.5.2, and watchOS 7.3.3 updates that patch the critical zero-day vulnerability

Apple just released a series of security updates aimed at addressing a relatively serious zero-day vulnerability on iOS.

This vulnerability is inherently actively exploited and affects many iPhone, iPad, iPod and Apple Watch devices around the world.

This vulnerability is tracked under the identifier CVE-2021-1879, It was first discovered and reported by cybersecurity experts Clement Lecigne and Billy Leonard, both from the Google Threat Analysis Group team. .

Google security experts have accidentally found this zero-day vulnerability in the Webkit iOS browser engine. According to the analysis, if successfully exploited, the vulnerability would allow malicious agents to perform a series of cross-site scripting attacks on multiple websites. But of course before that, they will have to deceive their target of opening malicious web content on their Apple devices.

The list of devices that may be affected by this vulnerability includes:

1. iPhone 6s or later, iPad Pro (all models), iPad Air 2 and up, iPad 5th generation or higher, iPad mini 4 or later, and iPod touch (7th generation).
2. iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch (6th generation).
3. Apple Watch Series 3 or later.

Immediately after receiving the notification of the vulnerability, Apple immediately embarked on the problem and soon released iOS 14.4.2, iOS 12.5.2 and watchOS 7.3.3 patches on March 28.

' *These updates come with important security patches and are recommended for all users,* ' Apple said in the update notice.

Seven zero-day vulnerabilities were patched within 5 months

Earlier, Apple also released a fix for two 'cluster' of zero-day vulnerabilities that were also actively exploited in iOS in January 2021 and November 2020. These vulnerabilities were reported by an Anonymous researcher and Project Zero - Google's zero-day bug hunting team.

Specifically, in January 2021, the Cupertino company fixed one bug in the iOS kernel (tracked as CVE-2021-1782) and two WebKit bugs (CVE-2021-1870 and CVE-2021-1871). In November 2020, Apple fixed three other zero-days on iOS - remote code execution bug (CVE-2020-27930), kernel memory leak (CVE-2020-27950), and privilege escalation error (CVE-2020-27932) - Affects iPhone, iPad and iPod devices.