Apple Rolls Out Zero-Day Patches to Older iOS, macOS Devices

Apple on Monday released updates for older versions of its iOS and macOS operating systems to patch zero-day vulnerabilities whose existence came to light last week.

The tech giant informed customers on Friday, April 7, that iOS and iPadOS 16.4.1 and macOS Ventura 13.3.1 patch CVE-2023-28206 and CVE-2023-28205, two zero-day vulnerabilities that can be exploited for arbitrary code execution. These updates are designed for the latest iPhones, iPads and Macs.

CVE-2023-28206 impacts the IOSurfaceAccelerator component and it can allow a malicious application to execute code with kernel privileges. CVE-2023-28205 affects WebKit and it can be exploited by luring the targeted user to a malicious website.

On Monday, Apple released iOS and iPadOS 15.7.5 to patch the vulnerabilities in iPhone 6s, iPhone 7, iPhone SE and older iPads. It also released macOS Monterey and Big Sur updates to fix CVE-2023-28206.

The vulnerabilities were reported to Apple by Google's Threat Analysis Group and Amnesty International's Security Lab. This suggests that the security holes have likely been exploited by commercial spyware vendors.

Google, Amnesty and Citizen Lab often disclose spyware attacks involving the exploitation of zero-day flaws.

Apple's iOS and macOS patches came a week after Google

detailed several zero-day and n-day vulnerabilities exploited by commercial spyware vendors to target Android and iOS devices.

The company, which tracks more than 30 spyware vendors, described Chrome, WebKit and kernel driver vulnerabilities exploited in sophisticated attacks whose goal is to hack into the devices of the targeted individuals.

Related: US to Adopt New Restrictions on Using Commercial Spyware

Related: Apple Patches Actively Exploited WebKit Zero-Day Vulnerability

Related: Apple Patches Zero-Day Vulnerability Exploited Against iPhones

Related: Apple Says WebKit Zero-Day Hitting iOS, macOS Devices

Apple Rolls Out Zero-Day Patches to Older iOS, macOS Devices