# Researchers uncover 23 critical vulnerabilities in Apple AirPlay affecting millions of devices



Cybersecurity researchers from Oligo Security have identified a significant number of vulnerabilities in Apple's AirPlay technology, which could potentially expose iPhones and other Apple devices to hacking if connected to compromised Wi-Fi networks. The research team discovered a total of 23 distinct security flaws, which they have collectively named ‘AirBorne’, reflecting the wireless nature of the attacks that can occur within the vicinity of the same network.

AirPlay is a feature allowing users to stream audio, video, and photos from their Apple devices to compatible smart appliances. However, the vulnerabilities could enable cybercriminals to execute various malicious actions, including stealing personal information, deploying harmful code, causing devices to crash, and even eavesdropping on private conversations.

Upon discovering these issues, Oligo Security promptly reported the vulnerabilities to Apple, leading to the launch of software updates on March 31 that addressed the issues for iPhones, iPads, Macs, and Apple Vision Pro devices. Apple confirmed to DailyMail.com that updates for affected third-party devices were also released and highlighted that the security vulnerabilities can only be exploited by attackers who are connected to the same Wi-Fi network as the targeted device.

Nevertheless, Oligo Security cautioned that certain third-party devices compatible with AirPlay may remain vulnerable if those device manufacturers do not issue timely software updates. Their Chief Technology Officer and co-founder, Gal Elbaz, pointed out that there are millions of third-party AirPlay-compatible devices that could still be susceptible to these vulnerabilities.

Elbaz also stated, "Because AirPlay is supported in such a wide variety of devices, there are a lot that will take years to patch — or they will never be patched," stressing the risk posed by vulnerabilities in a widely used piece of software. He indicated that if hackers gain access to a compromised device on the same Wi-Fi network, they could potentially infiltrate other connected devices.

To mitigate the risk of attacks, experts recommend that users ensure their devices are updated with the latest software releases. Additionally, disabling the AirPlay feature could provide an added layer of security, as it prevents the device from constantly broadcasting for signals in the background. Users can disable AirPlay by navigating to the Settings app, selecting 'General,' and then 'AirPlay & Continuity,' followed by selecting ‘Never’ under the ‘Automatically AirPlay’ tab.

As the cybersecurity landscape continues to evolve, the recommendation to regularly check for software updates on third-party devices employing AirPlay functionality is crucial for maintaining security against potential threats.

DailyMail.com has sought further comments from Apple regarding the ongoing situation.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.oligo.security/blog/critical-vulnerabilities-in-airplay-protocol-affecting-multiple-apple-devices> - This article from Oligo Security details the discovery of 23 vulnerabilities in Apple's AirPlay technology, collectively named 'AirBorne', which could expose Apple devices to hacking when connected to compromised Wi-Fi networks.
2. <https://support.apple.com/en-mk/122072> - Apple's official security content page for tvOS 18.3, released on January 27, 2025, addresses multiple AirPlay vulnerabilities, including CVE-2025-24126, CVE-2025-24129, CVE-2025-24131, and CVE-2025-24137, which were reported by Oligo Security.
3. <https://support.apple.com/en-uz/122066> - Apple's security content page for iOS 18.3 and iPadOS 18.3, released on January 27, 2025, lists AirPlay vulnerabilities CVE-2025-24126, CVE-2025-24129, CVE-2025-24131, CVE-2025-24177, and CVE-2025-24137, as reported by Oligo Security.
4. <https://support.apple.com/en-lamr/122073> - Apple's security content page for visionOS 2.3, released on January 27, 2025, addresses AirPlay vulnerabilities CVE-2025-24126, CVE-2025-24129, CVE-2025-24131, and CVE-2025-24137, reported by Oligo Security.
5. <https://bastille.net/critical-airplay-vulnerabilities-discovered/> - Bastille's article discusses the critical AirPlay vulnerabilities discovered by Oligo Security, highlighting the potential risks, including denial-of-service (DoS) attacks and remote code execution (RCE), which could allow attackers to gain unauthorized control over devices.
6. <https://9to5mac.com/2025/01/27/update-your-iphone-ipad-and-mac-now-to-fix-these-security-issues/> - 9to5Mac's article emphasizes the importance of updating iPhones, iPads, and Macs to the latest software versions to address security issues, including those related to AirPlay vulnerabilities identified by Oligo Security.
7. <https://www.dailymail.co.uk/sciencetech/article-14668521/iphone-users-warning-dangerous-flaws-turn-feature.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data