# Apple’s AirPlay protocol exposed to ‘AirBorne’ zero-click attacks affecting smart homes and enterprises



Apple users worldwide are facing a critical security alert following the identification of severe vulnerabilities in the AirPlay protocol, dubbed “AirBorne.” Researchers from the Tel Aviv firm Oligo have uncovered 23 significant flaws that could facilitate zero-click attacks, enabling hackers to remotely hijack devices and potentially steal sensitive data. As Apple issues urgent updates, the risks associated with these vulnerabilities have drawn widespread concern.

The AirPlay protocol, a cornerstone of Apple’s ecosystem designed for streaming audio and video from devices such as iPhones and iPads to compatible smart TVs and speakers, has become integral to many smart homes. However, this integration with a diverse range of third-party products, many of which may not receive timely security updates, has significantly broadened the potential attack surface. As Gal Elbaz, CTO of Oligo, emphasised, “Once a device is on the same Wi-Fi network as an attacker, it can be compromised without the user opening a link or even touching the screen.” This level of vulnerability is particularly alarming given that it affects not only consumer devices but also enterprise systems.

Those privy to Oligo's findings have highlighted that the AirBorne vulnerabilities could lead to a cascade of security issues, including memory corruption and buffer overflows, which could allow attackers to execute arbitrary code or install malware across networks. This could manifest in various ways, such as creating botnets of compromised devices, intercepting data streams, or even rendering devices inoperable. As Oligo's analysis outlines, the risks extend far beyond individual smartphones, threatening entire connected ecosystems within homes and businesses.

While Apple has promptly deployed fixes for its iPhones and other core devices, the situation regarding the plethora of third-party AirPlay-compatible devices remains precarious. Many of these devices, particularly older models, either lack adequate update mechanisms or are left vulnerable for extended periods, creating an ongoing risk for users. As noted in various discussions across tech platforms, including MacRumors, the inconsistency in security updates for third-party products underscores a growing concern: even as major platforms like Apple update systems, the broader network of connected devices can still leave users exposed.

To mitigate risks, Apple has provided guidance urging users to take immediate action. Users are encouraged to update their devices to the latest operating system versions and disable AirPlay receivers when not in use. Factors like using reputable security software to monitor network activity and avoiding connections to public or untrusted Wi-Fi networks are also advised. This incident is not an isolated concern for Apple; it highlights a recurring theme in cybersecurity — as devices become central to managing our digital lives, they increasingly represent gateways for broader attacks.

Moreover, this marks the second significant security challenge Apple has faced in recent months. Earlier this year, the company disclosed vulnerabilities pertaining to USB Restricted Mode, indicating that high-stakes security threats are becoming more pronounced within the ecosystem of Apple devices. Analysts suggest these patterns hint at a larger trend: as digital systems become more interconnected, vulnerabilities threaten to proliferate across a range of devices, necessitating enhanced vigilance from both manufacturers and users alike.

In light of the AirBorne vulnerabilities, it is imperative for users to remain informed and proactive about their digital security. Ensuring devices are updated and understanding the connectivity dynamics of smart devices can significantly reduce exposure to potential cyber threats, reinforcing the critical importance of vigilance in today's technology-driven landscape.

### Reference Map

1. Paragraph 1: 1, 2
2. Paragraph 2: 1, 3
3. Paragraph 3: 1, 5
4. Paragraph 4: 1, 3, 5
5. Paragraph 5: 1, 6, 7
6. Paragraph 6: 1, 5
7. Paragraph 7: 1, 4, 6

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

## Bibliography

1. <https://the420.in/iphone-airborne-hack-apple-security-warning-disable-airplay-now/> - Please view link - unable to able to access data
2. <https://www.oligo.security/blog/critical-vulnerabilities-in-airplay-protocol-affecting-multiple-apple-devices> - Oligo Security reports on critical vulnerabilities in Apple's AirPlay protocol, affecting devices like iPhones, iPads, Macs, and Apple TVs. The vulnerabilities, discovered in late 2024, could lead to Denial of Service (DoS) and Remote Code Execution (RCE) attacks, potentially allowing attackers to take control of affected devices or crash the AirPlay service. Users are advised to update their devices and disable the AirPlay receiver if not in use.
3. <https://www.macrumors.com/2025/04/29/airplay-vulnerabilities-third-party-devices/> - MacRumors discusses AirPlay security flaws impacting both Apple and third-party devices. Researchers at Oligo identified vulnerabilities that could allow attackers to control AirPlay-enabled devices over local Wi-Fi networks without user interaction. Apple has addressed these flaws in recent security updates, but many third-party devices remain vulnerable due to delayed or absent patches.
4. <https://www.oligo.security/blog/airborne> - Oligo Security provides an in-depth analysis of the 'AirBorne' vulnerabilities in Apple's AirPlay protocol. The vulnerabilities enable zero-click Remote Code Execution (RCE) attacks, allowing malware to spread across devices without user interaction. The blog details the technical aspects of the vulnerabilities and recommends immediate updates and disabling of the AirPlay receiver on devices not in active use.
5. <https://tribune.com.pk/story/2543771/apples-airplay-vulnerability-airborne-risks-iphones-macs-and-more> - The Express Tribune reports on Apple's AirPlay vulnerability, known as 'AirBorne,' which poses risks to iPhones, Macs, and other devices. Despite Apple's March 2025 security updates, many third-party products remain unpatched, leaving millions of devices exposed. Experts warn that hackers can exploit these vulnerabilities to execute malicious code, steal sensitive information, and cause device malfunctions.
6. <https://secure-iss.com/soc-advisory-apple-airplay-zero-click-rce-vulnerability-airborne-29-april-2025/> - Secure-ISS provides a Security Operations Center (SOC) advisory on the 'AirBorne' zero-click Remote Code Execution (RCE) vulnerability in Apple's AirPlay protocol. The advisory details the affected versions, including iOS 18.4, iPadOS 18.4, macOS Ventura 13.7.5, and others. It outlines the exploitation methods and recommends immediate patching, disabling the AirPlay receiver, and network hardening measures.
7. <https://basefortify.eu/posts/2025/05/apple_airplay_under_siege%3A_unpacking_airborne%E2%80%99s_wormable_zero-click_exploits.html> - BaseFortify discusses the 'AirBorne' vulnerabilities in Apple's AirPlay protocol, highlighting the risks of zero-click Remote Code Execution (RCE) attacks. The article explains how these vulnerabilities allow malware to spread across devices without user interaction and provides technical insights into the exploitation methods. It emphasizes the importance of updating devices and securing network configurations to mitigate the risks.