# AirBorne vulnerabilities expose over 2 billion devices to remote hacking via AirPlay



Recent security findings have raised alarms for users of Apple's AirPlay protocol, revealing a significant number of vulnerabilities, collectively dubbed "AirBorne." Researchers from Oligo Security uncovered 23 critical flaws that could potentially enable hackers to compromise a range of devices, including iPhones, Macs, smart speakers, and even vehicles equipped with CarPlay. Given the pervasive use of AirPlay in over 1.8 billion active iPhones alone, and approximately 500 million additional AirPlay-compatible devices globally, the implications of these vulnerabilities are extensive, posing a serious risk to millions.

The vulnerabilities identified by Oligo Security include various exploits that could lead to remote code execution, a scenario in which attackers can commandeer devices without requiring any interaction from users. Particularly worrying are the zero-click attacks, which allow for breaches without any visible indication that anything is amiss. For example, one such malicious exploit can involuntarily replace legitimate applications, such as Apple Music, with harmful software.

Apple has taken steps to mitigate these threats, releasing security patches on March 31 that include updates for iOS 18.4, macOS Sequoia 15.4, and tvOS 18.4. However, the situation remains precarious for numerous third-party devices that utilise AirPlay technology. Experts caution that while Apple’s latest updates address vulnerabilities in its own products, many manufacturers of compatible devices have yet to provide timely fixes. As Elbaz from Oligo pointed out, certain AirPlay-compatible devices may take years to receive necessary patches, if they receive them at all.

The nature of the AirBorne vulnerabilities can lead to harmful consequences that extend beyond individual devices. By leveraging these flaws, attackers could deploy malware that propagates across local networks, akin to a network worm. This behaviour highlights the urgent need for vigilance among users, especially when using AirPlay on public networks. The recommended course of action includes disabling AirPlay when not in use and limiting access to trusted users only.

Apple maintains that exploitation of these vulnerabilities would require an attacker to be on the same Wi-Fi network as the targeted device. However, the breadth of the threat landscape remains daunting. Oligo’s findings suggest that the interconnectedness of various devices means a breach on one could facilitate broader attacks across an entire network. Cybersecurity experts advise users to exercise caution, particularly regarding third-party devices, which might not enjoy the same level of scrutiny or support as Apple’s native products.

To secure their devices, users are encouraged to ensure that all software is regularly updated and to disable unnecessary features, such as AirPlay receivers, which continuously broadcast and listen for connections, presenting an “attack surface” that hackers can exploit. Disabling AirPlay can significantly reduce the risk of unauthorized access.

As the number of connected devices continues to rise, so does the likelihood of encountering vulnerabilities. Therefore, it is vital for users to remain proactive in their digital security practices. The risk is not isolated to Apple devices alone; the interconnected nature of technology means that vulnerabilities in one system can have cascading effects on others. By adopting a more cautious approach to technology usage, users can better protect themselves against the threats posed by the AirBorne vulnerabilities and similar exploits in the future.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5
2. Paragraphs 1, 2
3. Paragraphs 2, 3
4. Paragraphs 1, 3, 4
5. Paragraph 1, 5

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

## Bibliography

1. <https://www.dailymail.co.uk/sciencetech/article-14728593/Urgent-warning-iPhone-auto-feature-NOW.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.wired.com/story/airborne-airplay-flaws/> - Researchers from Oligo Security have identified a series of vulnerabilities in Apple's AirPlay protocol, collectively termed 'AirBorne.' These flaws could allow attackers to remotely hijack AirPlay-enabled devices, including speakers, receivers, and smart TVs, provided they are on the same Wi-Fi network. The vulnerabilities also pose risks to CarPlay systems in vehicles. Apple has released patches for its devices, but many third-party devices may remain vulnerable due to delayed updates. Users are advised to update their devices and exercise caution when using AirPlay on public networks. ([wired.com](https://www.wired.com/story/airborne-airplay-flaws/?utm_source=openai))
3. <https://www.techrepublic.com/article/news-apple-airplay-airborne-vulnerabilities/> - Security researchers have discovered 23 vulnerabilities in Apple's AirPlay protocol, collectively known as 'AirBorne.' These flaws could enable remote code execution attacks, allowing hackers to take control of Apple and third-party devices over a local network without user interaction. The vulnerabilities include zero-click and one-click exploits, access control list bypasses, and denial-of-service attacks. Apple has released security updates to address these issues, but third-party devices may remain exposed if manufacturers do not provide timely patches. Users are urged to update their devices and restrict AirPlay access to trusted users. ([techrepublic.com](https://www.techrepublic.com/article/news-apple-airplay-airborne-vulnerabilities/?utm_source=openai))
4. <https://www.oligo.security/blog/airborne> - Oligo Security has detailed the 'AirBorne' vulnerabilities in Apple's AirPlay protocol, which expose devices to multiple attacks, including zero-click remote code execution and denial-of-service exploits. The vulnerabilities stem from issues in the AirPlay Software Development Kit (SDK) used by Apple and third-party manufacturers. Apple has released patches for its devices, but many third-party devices may remain vulnerable due to delayed updates. Users are advised to update their devices and disable AirPlay receivers when not in use to mitigate potential risks. ([oligo.security](https://www.oligo.security/blog/airborne?utm_source=openai))
5. <https://www.macworld.com/article/2768062/the-airplay-device-connected-to-your-iphone-or-mac-may-be-a-target-for-hackers.html> - Macworld reports on vulnerabilities in Apple's AirPlay protocol that could allow hackers to gain control of AirPlay-enabled devices. The flaws, discovered by Oligo Security, have been patched in Apple's devices, but third-party products may remain exposed if manufacturers do not provide software updates. Users are advised to update their devices and disable AirPlay reception when not in use to enhance security. ([macworld.com](https://www.macworld.com/article/2768062/the-airplay-device-connected-to-your-iphone-or-mac-may-be-a-target-for-hackers.html?utm_source=openai))
6. <https://secure-iss.com/soc-advisory-apple-airplay-zero-click-rce-vulnerability-airborne-29-april-2025/> - Secure-ISS provides an advisory on the 'AirBorne' zero-click remote code execution vulnerability in Apple's AirPlay protocol. The vulnerability allows attackers on the same Wi-Fi network to execute code on affected devices without user interaction. Apple has released security updates to address the issue, but third-party devices may remain vulnerable if manufacturers do not provide timely patches. Users are advised to update their devices and disable AirPlay receivers when not in use. ([secure-iss.com](https://secure-iss.com/soc-advisory-apple-airplay-zero-click-rce-vulnerability-airborne-29-april-2025/?utm_source=openai))
7. <https://www.apfelpatient.de/en/news/airplay-security-vulnerabilities-what-you-need-to-know-now> - Apfelpatient discusses the 'AirBorne' vulnerabilities in Apple's AirPlay protocol, which allow attackers to gain access to AirPlay-enabled devices via a shared Wi-Fi network. The vulnerabilities can be exploited individually or in combination, leading to various attacks such as remote code execution and denial-of-service. Apple has released security updates to address these issues, but many third-party devices may remain vulnerable due to delayed updates. Users are advised to update their devices and disable AirPlay receivers when not in use. ([apfelpatient.de](https://www.apfelpatient.de/en/news/airplay-security-vulnerabilities-what-you-need-to-know-now?utm_source=openai))