Zero-Click, Wormable RCE Found in Apple AirPlay – Millions of Devices Vulnerable

Overview

TL;DR

Attackers can break into Apple and third-party devices using AirPlay over Wi-Fi. Update now.

A new set of vulnerabilities in Apple's AirPlay protocol, referred to as AirBorne, introduces the risk of wormable, zero-click remote code execution (RCE) across a range of Apple and third-party devices. If exploited, these flaws could allow attackers on the same Wi-Fi network to hijack devices without user interaction. Attackers could also install malware and move laterally within an environment.

Vulnerability Breakdown

- CVE-2025-24252 (CVSS 9.8) and CVE-2025-24206 (CVSS 7.7) – Used together, these allow attackers to run code on a Mac without any user interaction.
- CVE-2025-24132 (CVSS 6.5) – Targets smart speakers and TVs; attacker can take control without any clicks.
- CVE-2025-24271 (CVSS 5.4) – Lets anyone on the same network send AirPlay commands to a Mac.
- Others (like CVE-2025-24137, CVE-2025-24251, CVE-2025-31197, CVE-2025-30445, CVE-2025-31203) can crash apps, leak data, or shut down devices.

Third-party devices that use Apple's AirPlay SDK, like smart TVs and set-top boxes, are just as exposed. Many of these won't get patched anytime soon.

What is Impacted?

- iPhones, iPads, and Macs running outdated software
- Smart TVs, speakers, and home media devices with AirPlay
- Car infotainment systems using CarPlay
- Corporate laptops or devices that connect to public Wi-Fi

This is a classic example of convenience turning into exposure. AirPlay was designed to make devices talk to each other easily, but that same openness is now a problem. Not

updating the devices mentioned above leaves you exposed. Aspire recommends that you update as soon as possible.

Aspire Protects

- **Patch –** Update all Apple devices immediately. You can view a complete list of links to updates via Oligo Security's blog post. Patched versions include:
  - iOS 18.4 and iPadOS 18.4
  - iPadOS 17.7.6
  - macOS Sequoia 15.4
  - macOS Sonoma 14.7.5
  - macOS Ventura 13.7.5
  - tvOS 18.4, and
  - visionOS 2.4
- Disable the AirPlay receiver if it is not in use.
- Push updates to any AirPlay enabled devices on your network, including smart TVs and speakers.
- Avoid using public Wi-Fi with AirPlay turned on.

TTPs to Watch

Execution

- Exploitation for Client Execution [T1203] – The attacker may exploit AirPlay flaws to run malicious code silently.

Lateral Movement

- Internal Spearphishing [T1534] – Once inside, the infected device could be used to target others on the same network.

Command and Control

- Application Layer Protocol [T1071.001] – Malware could use standard protocols to stay connected and move data.

Persistence

- Valid Accounts [T1078] – Compromised devices could help attackers collect credentials or maintain access to internal systems.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how

we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Any business using Apple hardware or smart devices, especially those in:

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government
- Energy

Risk goes up if your place of business connects to public Wi-Fi, travels with devices, or uses smart displays in meeting spaces.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will

ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Apple security releases - Apple Support

Airborne: Wormable Zero-Click RCE in Apple AirPlay Puts Billions of Devices at Risk | Oligo Security | Oligo Security