Исследователи из Oligo Security раскрыли набор уязвимостей в протоколе AirPlay от Apple, получивший название “AirBorne”. Эти недостатки позволяют хакерам, подключенным к той же Wi-Fi-сети, захватывать контроль над устройствами с поддержкой AirPlay, включая iPhone, Mac, умные колонки и телевизоры, без ввода пароля. Об этом пишет Security Affairs.

AirPlay — технология Apple для беспроводной передачи аудио, видео и другого контента между устройствами. Уязвимости затрагивают как устройства Apple, так и сторонние продукты, использующие AirPlay SDK. Хакеры могут выполнять удаленный код (RCE), что позволяет запускать вредоносное ПО, шпионить через микрофоны или распространять вирусы. Проблема также затрагивает CarPlay, но для атаки требуется физическое подключение через Bluetooth или USB.

Apple выпустила патчи для своих устройств (iOS 18.4, macOS 15.4), но миллионы сторонних устройств остаются уязвимыми, так как их обновления зависят от производителей. Oligo советует пользователям обновлять устройства, отключать AirPlay на неиспользуемых гаджетах и избегать публичных Wi-Fi.