

Apple выпустила новые обновления для своих операционных систем, исправив уязвимости, которые активно использовались злоумышленниками. Это включает важные исправления для старых версий ОС, которые ранее были обновлены только в более новых релизах.

Одной из самых критичных уязвимостей является CVE-2025-24 200, связанная с функцией USB Restricted Mode, которая была введена еще в 2018 году. Она блокирует порты Lightning или USB-C, если устройство заблокировано более часа. Уязвимость позволяла хакерам с физическим доступом к устройству отключать эту функцию безопасности, что могло привести к утечке данных. Эта ошибка была устранена в iOS 18.3.1 и iPadOS 18.3.1, а теперь также исправлена в версиях iOS 16.7.11 и 15.8.4, а также в соответствующих версиях iPadOS.

Кроме того, была исправлена еще одна уязвимость (CVE-2025-24 201), которая позволяла вредоносным контентам обходить защиту в Safari. Эти исправления также поступили в версии iOS 16.7.11 и 15.8.4 и соответствующие версии iPadOS.

Для macOS Ventura была выпущена версия 13.7.5, которая исправляет уязвимость в CoreMedia, используемую для повышения привилегий. Кроме того, обновления были выпущены для macOS Sonoma (версия 14.7.5), которая включает 90 патчей, и для macOS Sequoia (версия 15.4), которая получила более 120 исправлений.