

Найдена Bluetooth-дыра в наушниках Sony, JBL и Bose — возможен перехват звонков и взлом устройства

Исследователи компании ERNW выявили критические уязвимости в Bluetooth-чипах Airoha, используемых в 29 аудиоустройствах от Sony, JBL, Bose, Marshall, Jabra и других брендов. Об этом они сообщили на конференции TROOPERS в Германии.

Уязвимости позволяют хакерам в пределах Bluetooth-дальности перехватывать текущие аудиотреки, инициировать звонки и даже извлекать список контактов и историю вызовов с телефона жертвы.

В некоторых случаях возможно и прослушивание разговоров вместе с перепрошивкой наушников с дальнейшим удалённым выполнением кода.

Наиболее опасная из уязвимостей — CVE-2025-20702 — получила оценку 7.5 по шкале CVSS. Эксплуатация требует высокой квалификации и физической близости к цели, что ограничивает риск массовых атак, но создаёт угрозу для высокопрофильных лиц, таких как журналисты и дипломаты.

Компания Airoha выпустила обновлённый SDK, но, по данным Heise, прошивки большинства устройств пока не обновлены. Пользователям рекомендовано проверять наличие новых версий ПО для своих наушников.