CÔNG CỤ BẺ KHÓA BLUETOOTH ĐƯỢC CÔNG KHAI

Các lậ

Các lập trình viên người Đức vừa công bố mã xâm nhập thiết bị Bluetooth thông qua một lỗ hổng của chuẩn này. Theo đó, ngay cả khi người dùng bật tính năng bảo mật, họ vẫn bị nghe lén và chiếm quyền điều khiển điều khiển thiết bị.

Giới chuyên gia vừa có cuộc gặp gỡ tại đại hội truyền thông Chaos diễn ra ở Berlin (Đức) để thảo luận về 2 công cụ tấn công thiết bị dùng chuẩn liên lạc không dây tầm gần Bluetooth (gồm cả máy tính). Mục đích của họ là nhằm cảnh báo lỗ hổng an ninh vốn rất ít được quan tâm này.

Theo Thierry Zoller, người giới thiệu công cụ đồng thời là một tư vấn viên bảo mật, các doanh nghiệp thường bỏ qua vấn đề anh toàn cho Bluetooth và họ cần nhận thức được yếu kém cơ bản trong chuẩn không dây.

Chương trình BTCrack được Zoller phát triển để khai thác lỗ hổng biết tới từ năm 2005, lợi dụng yếu kém trong mã PIN của thiết bị Bluetooth, cho phép kẻ tấn công nghe lén và truy cập vào máy của khổ chủ, cả đầu gọi lẫn đầu nhận, ngay cả khi rào chắn an ninh đã bật lên.

Còn HID Attack là công cụ chiếm quyền điều khiển bàn phím Bluetooth dùng chuẩn HID, cho phép truy cập vào các hệ thống nhạy cảm. "Tôi nhận ra vấn đề này khi đang phát triển một phím phần mềm", Collin Mulliner, người viết sản phẩm này, cho biết. "Nguy cơ của nó là rất lớn vì kẻ tấn công có thể tiếp cận vào hệ thống đầu cuối".

Việc tấn công thiết bị này không dễ dàng vì khi hacker truy cập vào máy, màn hình sẽ sáng lên khiến người dùng nghi ngờ và có thể tắt Bluetooth. Tuy nhiên, các bước tiến trong việc khai thác lỗ hổng của chuẩn này buộc các chuyên gia phải tìm giải pháp an toàn hơn.