

TÌM THẤY LỖI WIFI TRONG LINUX

Một lỗ

Một lỗi đã được tìm thấy trong bộ điều khiển WiFi Linux, nó có thể cho phép kẻ tấn công chiếm được quyền kiểm soát laptop thậm chí cả khi không còn kết nối vào mạng WiFi nữa.

Không có nhiều bộ điều khiển thiết bị Linux WiFi bị lỗi này và hình như mới chỉ có thực thi được từ xa lỗi WiFi này. Nó tác động nhiều lên mạng sử dụng driver thiết bị nhận MadWiFi Linux cho các chip nền tảng Atheros WiFi, theo như nhà nghiên cứu Laurent Butti từ France Telecom Orange nói, đó cũng là người đã tìm ra lỗ hổng và đưa thông tin trong hội nghị Black Hat tháng trước tại Amsterdam.

"Bạn có thể bị tấn công nếu không tự có bản vá tạm trong driver MadWiFi", Butti cảnh báo. Trước khi công bố rộng rãi lỗ hổng này, Butti đã đưa ra lỗ hổng này cho nhóm phát triển MadWiFi và họ sẽ công bố một bản vá. Tuy nhiên không phải tất cả các phân phối Linux đều có thể xây dựng bản vá bên trong mã của họ, Butti nói.

Lỗi tràn ngăn xếp nhân có thể cho phép kẻ tấn công chạy mã độc hại và sử dụng máy tính thậm chí cả khi không còn hoạt động trong mạng WiFi nữa, Butti cảnh báo. Butti đã sử dụng kỹ thuật test "fuzzing" để phát hiện ra lỗ hổng. Kỹ thuật này đã được biểu diễn bởi David Maynor và "Johnny Cache" Jon Elch tại hội nghị Black Hat USA vào năm ngoái và trước đây đã thành công trong hệ thống Windows và Macintosh.

Với một vài laptop Linux trên mạng WiFi, các chuyên gia bảo mật - và có thể cả hacker - đã kiểm tra toàn bộ các driver Linux. Kết quả của quá trình điều khiển từ xa dữ liệu trong mức nhân có thể là nguyên nhân sự cố trong hệ điều hành nguồn mở này cũng dễ dàng như bất kỳ hệ thống nào.

Butti trước đây đã phát triển một loạt RAW làm minh chứng cơ sở cho các công cụ hacker. Ông đã tìm thấy lỗi hổng WiFi trong Windows bằng kỹ thuật fuzzing trong suốt Tháng lỗi nhân vào năm ngoái.

Butti nói, kỹ thuật Fuzzing là hoàn hảo bởi nó phương pháp tốn ít giá thành giúp các chuyên gia bảo mật khám phá ra những lỗ hổng không nhìn thấy nhưng lại bị hacker khai thác. Trong tương lai, ông hy vọng fuzzing sẽ phát hiện ra các lỗ hổng trong công nghệ mạng không dây như WiMax và USB không dây. Sẽ có nhiều lỗ hổng hơn nữa được phát hiện trong quá trình mở rộng WiFi.

