LAPTOP DELL, HP MẮC LỖI BẢO MẬT WI-FI

Các ch

Các chuyên gia phân tích bảo mật hiện đang cảnh báo người dùng về một lỗi bảo mật nghiêm trọng trong trình điều khiển thiết bị không dây Wi-Fi Broadcom tích hợp trong các dòng sản phẩm của HP, Dell, Gateway và eMachines.

Lỗi bảo mật Wi-Fi mới được phát hiện là một lỗi tràn bộ nhớ đệm nằm trong phần mềm trình điều khiển thiết bị không dây Broadcom, phát sinh khi xử lý các gói dữ liệu mạng không dây 802.11 có chứa các trường SSID quá dài.

Lỗi này có thể bị khai thác để từ xa thực thi các mã nhị phân ở chế độ nhân hệ thống, chiếm toàn bộ quyền điều khiển các loại máy tính xách tay có tích hợp tính năng Wi-Fi mắc lỗi.

Tuy nhiên, ZERT (Zero Day Emergency Response Team) cho biết kẻ tấn công chỉ có thể khai thác lỗi bảo mật nếu hệ thống mắc lỗi nằm trong vùng phủ sóng Wi-Fi cùng với kẻ tấn công.

Mức độ nguy hiểm của lỗi bảo mật này càng tăng cao khi mà hệ điều hành Windows có cài đặt trình điều khiển Wi-Fi Broadcon mắc lỗi có thể bị khai thác lỗi ngay cả khi gần đó không có điểm hot-spot Wi-Fi nào và không cần bất cứ một sự tương tác nào từ phía người dùng đầu cuối.

Lỗi bảo mật Wi-Fi Broadcom là thành quả của dự án “Tháng của các lỗi nhân” do H.D. Moore khởi động.

Jon "Johnny Cache" Ellch là người đầu tiên phát hiện những lỗi bảo mật Wi-Fi tương tự như trên. Lỗi này lần đầu tiên được công bố tại diễn đàn Blue Hat của Microsoft hồi tháng 10 vừa qua. Sản phẩm đầu tiên bị phát hiện mắc lỗi là trình điều khiển Wi-Fi trong Mac OS X trên các dòng laptop của Apple.

Ellch đã cảnh báo về lỗi bảo mật trong trình điều khiển Wi-Fi Broadcon ngay từ đầu năm 2006 và chờ đợi nhà sản xuất tung ra bản vá lỗi. Song song bên cạnh đó ông cũng hợp tác với dự án Metasploit của H.D. Moore để phát triển một mô-đun mã tấn công lỗi nói trên đến bổ sung vào các công cụ thử nghiệm lỗi bảo mật.

Tính đến thời điểm này thì Broad đã phát hành bản cập nhật bảo mật vá lỗi bảo mật nói trên. Tuy nhiên, số lượng người dùng cài đặt bản vá lỗi còn tương đối ít.

Hoàng Dũng