PHƯƠNG THỨC TẤN CÔNG MỚI NHẮM VÀO ROUTER VÀ ĐTDĐ

Một ch

Một chuyên gia bảo mật tại Juniper Networks vừa phát triển một phương pháp tấn công mới cho phép chạy các chương trình bất hợp pháp trên hàng loạt các thiết bị máy tính, trong đó có cả router và điện thoại di động.

Tại hội nghị bảo mật CanSecWest được tổ chức ở Vancouver ngày 19/4, chuyên gia Barnaby Jack đã trình diễn cách thức kiểm soát router và chèn phần mềm độc hại vào tất cả các máy tính trong một mạng.

Jack cho biết anh đã phát hiện phương pháp mới cho phép biến một lỗi thường thường trong máy tính - lỗi xoá tham chiếu trỏ chuột rỗng thành một thứ nguy hiểm hơn gấp nhiều lần so với những gì được biết tới trước đây.

Cho tới nay, lỗ trỏ chuột rỗng vẫn không được coi là nghiêm trọng mặc dù nó có thể khiến máy tính bị treo nhưng lại không gây ra bất cứ một thiệt hại nghiêm trọng nào. Trong nhiều năm qua, các nhà nghiên cứu bảo mật đã từng biết tới lỗ hổng dạng này, xảy ra khi máy tính thông báo cho một chương trình rằng một phần bộ nhớ mà chúng đang tìm kiếm không tồn tại, hoặc "rỗng".

Tuy nhiên, tại buổi trình diễn ngày 19/4, Jack tuyên bố lỗ hổng trỏ chuột rỗng có thể cho phép chạy những phần mềm bất hợp pháp trên nhiều loại thiết bị máy tính. Kỹ thuật mới này được Jack mô tả là "đáng tin cậy 100% và có khả năng thực thi mã trên thiết bị".

Tuy nhiên, mã khai thác lỗi trỏ chuột rỗng của Jack hiện mới chỉ hoạt động trên nền tảng bộ xử lý Arm và xScale (đang được sử dụng rộng rãi cho các thiết bị gắn kèm), chứ chưa thể thực hiện được trên kiến trúc Intel.