

PHÁT HIỆN LỖ HỔNG BẢO MẬT NGHIÊM TRỌNG TRONG... MICROCHIP

Các nh

Các nhà nghiên cứu vừa tìm thấy một lỗ hổng trọng yếu bên trong công nghệ vi xử lý, có thể cho phép hacker moi được những thông tin tuyệt mật của người dùng máy tính.

Thông tin đăng tải trên nhật báo Le Monde của Pháp hôm thứ bảy vừa qua cho hay nhóm nghiên cứu của chuyên gia mã hóa Jean-Pierre Seifert nhận thấy các con chip ngày nay hớ hênh hơn nhiều so với trước đây. Nguyên nhân nằm ở công nghệ sản xuất ra chúng, khi các hãng muốn vi chip xử lý dữ liệu nhanh hơn.

Nguồn: xtmedia

"Bảo mật đã bị hy sinh để đổi lấy hiệu suất", Seifert cho biết.

Trên thực tế, đây không phải là lần đầu tiên người ta đề cập đến nguy cơ hacker đột nhập vào trong chip máy tính nhờ kỹ thuật có tên Phân tích dự đoán nhánh (PBA). Tuy nhiên kỹ thuật này đòi hỏi bọn chúng phải thử qua rất nhiều dãy số trước khi giải mã được chìa khóa mã hóa.

Tuy nhiên, nghiên cứu mới nhất của Seifert cho thấy hacker sẽ tấn công vào vi xử lý dễ dàng, nhanh chóng hơn nhiều chỉ với một phần mềm do thám đặc biệt, chuyên giám sát các vi chip.

Seifert và các đồng sự đã giải thích cặn kẽ cách họ có thể tìm được chìa khóa mã 512-bit chỉ sau một lần thử duy nhất bên trong công trình nghiên cứu chưa được công bố này.

Theo dự kiến, ông Seifert sẽ trình bày phương pháp giải mã của mình vào đầu năm tới, trong một cuộc hội thảo quốc tế về mã hóa.

Trọng Cẩm