TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Phát hiện lỗ hổng bảo mật nghiêm trọng tồn tại trên chip xử lý Intel

16:24 16/05/2019

Thông tin Cục An toàn thông tin, Bộ Thông tin và Truyền thông (TT&TT) vừa phát đi cảnh báo đến người dùng lỗ hổng bảo mật trong các thiết bị máy tính để bàn, máy tính xách tay, máy chủ, điện thoại di động đang sử dụng bộ vi xử lý Intel.

Trong nội dung phát đi, Cục An toàn thông tin cho biết các chuyên gia về an toàn thông tin thuộc Đại học Công nghệ Graz của Áo và Đại học Công giáo Leuven của Bỉ đã công bố một nhóm bao gồm 4 điểm yếu an toàn thông tin trong bộ vi xử lý Intel.

Cụ thể, 4 điểm yếu an toàn thông tin có mã lỗi quốc tế là: CVE-2018-12126; CVE-2018-12130; CVE-2018-12127; CVE-2019-11091. Các điểm yếu an toàn thông tin này được các chuyên gia đánh giá là nghiêm trọng và có ảnh hưởng tới nhiều thiết bị đang sử dụng bộ vi xử lý của Intel bao gồm: máy tính để bàn, máy tính xách tay, máy chủ, điện thoại di động sử dụng các hệ điều hành Linux, Windows, MacOS, Android ...



Phát hiện lỗi bảo mật nghiêm trọng tồn tại trên chip xử lý Intel (Ảnh minh họa)

Các hình thức tấn công lợi dụng 4 điểm yếu an toàn thông tin trên được các chuyên gia công bố và vẫn đang được tiếp tục nghiên cứu, đánh giá sâu hơn bao gồm: Tấn công ZombieLoad sử dụng điểm yếu CVE-2018-12130; Tấn công RIDL sử dụng điểm yếu CVE-2018-12127 và CVE-2019-11091; Tấn công Fallout sử dụng điểm yếu CVE - 2018-12126.

Hiện tại Intel đã công bố danh sách sản phẩm bị ảnh hưởng và kế hoạch cập nhật, đồng thời làm việc với các doanh nghiệp sản xuất hệ điều hành, firmware, thiết bị để hỗ trợ cập nhật bản vá.

Trước tình hình nói trên, để bảo đảm an toàn thông tin và phòng tránh việc đối tượng tấn công lợi dụng điểm yếu an toàn thông tin để thực hiện những cuộc tấn công mạng nguy hiểm, Cục An toàn thông tin khuyến nghị các quản trị viên tại các cơ quan, đơn vị và người dùng thự hiện các thao tác nhằm đảm bảo an toàn.

Cụ thể, người dùng cần kiểm tra, rà soát, xác định các máy tính bị ảnh hưởng bởi các điểm yếu trên; Cập nhật bản vá hoặc nâng cấp các hệ điều hành để tạm thời vá các điểm yếu.

Đối với các hệ điều hành chưa có thông tin về bản vá, cần theo dõi thường xuyên để nâng cấp ngay khi có biện pháp xử lý. Đối với những dòng sản phẩm

mà Intel không có kế hoạch cập nhật cần lên kế hoạch thay thế trong thời gian tới. Thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin nhằm đối phó kịp thời với các nguy cơ tấn công mạng.

Trong trường hợp cần thiết, có thể liên hệ Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin, số điện thoại: 024.3209.1616, thư điện tử ais@mic.gov.vn hoặc Fanpage của NCSC theo đường dẫn https://www.facebook.com/govSOC/ để được hỗ trợ kịp thời.

Cục An toàn thông tin cũng cho biết đang tiếp tục theo dõi, nghiên cứu để đưa ra các hướng dẫn chi tiết. Các thông tin này sẽ được Cục An toàn thông tin cập nhật trên hệ thống chia sẻ thông tin (https://ti.khonggianmang.vn).

Ngọc Lan