BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 541/CATTT-TĐQLGS
V/v cảnh báo nguy cơ mất an toàn thông tin trên các thiết bị sử dụng mạng Wi-Fi

Hà Nội, ngày 16 tháng 10 năm 2017

Kính gửi:

Ngày 16 tháng 10 trên trang web của nhà nghiên cứu bảo mật Mathy Vanhoef (www.krackattacks.com) đã công bố một nhóm lỗ hổng trong giao thức WPA/WPA2, một giao thức được coi là an toàn nhất cho mạng không dây (Wi-Fi) hiện nay cho phép thực hiện kỹ thuật tấn công KRACKs (Key Reinstallation Attacks). Cụ thể, đối tượng tấn công có thể nghe lén, giải mã giao thức mã hóa và đọc được nội dung của các gói tin mà trước đây được cho là an toàn. Lỗ hổng này có thể bị lợi dụng để đánh cắp các thông tin cá nhân, thông tin nhạy cảm như tài khoản ngân hàng, thẻ tín dụng, tài khoản mạng xã hội, tài khoản trực tuyến, thông tin riêng, nội dung chat, thư điện tử, hình ảnh, video…được truyền qua mạng không dây.

Lỗ hổng này tồn tại trong chính nội tại của giao thức mạng không dây Wi-Fi chứ không liên quan đến các sản phẩm hay cách thức triển khai mô hình mạng, bất cứ thiết bị mạng không dây nào sử dụng giao thức mã hóa WPA/WPA2 đều có thể là mục tiêu của hình thức tấn công. Theo đánh giá, các thiết bị Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys và nhiều thiết bị khác cũng có thể bị tấn công bằng việc điều chỉnh cách thức tấn công KRACKs cho phù hợp.

Hình thức tấn công này ảnh hưởng đến tất cả các thiết bị phát sóng Wi-Fi sử dụng giao thức WPA/WPA2. Và tùy thuộc vào cấu hình của hệ thống mạng, đối tượng tấn công thậm chí còn có thể thay đổi nội dung gói tin, hay đính kèm mã độc tống tiền, mã độc gián điệp vào các gói tin và để người dùng tự lây nhiễm.

Nhằm bảo đảm an toàn thông tin và phòng tránh việc đối tượng tấn công lợi dụng lỗ hổng để thực hiện những cuộc tấn công mạng nguy hiểm, Cục ATTT khuyến nghị các quản trị viên tại các cơ quan, đơn vị và người dùng thực hiện:

Đối với người dùng:

- Lỗ hổng trên các thiết bị phát sóng không dây khó có thể sẽ có bản vá ngay lập tức, vì vậy cần thường xuyên theo dõi các bản cập nhật trên các thiết bị cầm tay, các thiết bị di động, trình điều khiển card mạng không dây của máy tính và các thiết bị phát sóng Wi-Fi để cập nhật ngay khi có các bản vá mới.

- Luôn cẩn trọng khi sử dụng các mạng không dây đặc biệt là các mạng không dây công cộng, chỉ truy cập các trang web sử dụng giao thức bảo mật HTTPS và thận trọng khi nhập thông tin các tài khoản cá nhân, hay các thông tin nhạy cảm khác trên các trang web.

- Tiếp tục duy trì giao thức mã hóa WPA/WPA2 cho các thiết bị phát sóng không dây sử dụng tại gia đình kết hợp với mật mã ở mức độ khó cao, do đây vẫn là giao thức mã hóa an toàn nhất hiện nay ngăn chặn được các hình thức tấn công giải mã khác.

Ngoài ra đối với cơ quan, tổ chức:

- Cảnh báo tới người dùng trong tổ chức và thực hiện các biện pháp như nêu trên đối với người dùng;

- Chủ động theo dõi các thông tin từ các cơ quan chức năng và các tổ chức về an toàn thông tin để kịp thời cập nhật các bản vá cho các thiết bị mạng của mình, đồng thời đôn đốc các cán bộ đang làm việc trong cơ quan, tổ chức chủ động thường xuyên theo dõi và cập nhật các thiết bị đầu cuối khi có bản cập nhật mới.

- Liên hệ ngay với các cơ quan chức năng cũng như các tổ chức, doanh nghiệp trong lĩnh vực an toàn thông tin để được hỗ trợ khi cần thiết.

Khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Cục An toàn thông tin, số điện thoại: 04.3943.6684, thư điện tử ais@mic.gov.vn để được phối hợp, hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Cục trưởng (để b/c);
- Cơ quan đơn vị thuộc Bộ;
- Lưu: VT, TĐQLGS.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

(đã ký)

Nguyễn Huy Dũng