BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

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

Số: 219 / VNCERT-KTHT

Hà Nội, ngày 10 tháng 10 năm 2014

V/v cảnh báo nguy cơ mất an toàn thông tin từ lỗi của thiết bị lưu trữ USB

Kính gửi:
- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW.

Tại hội nghị hacker Black Hat tháng 8/2014 tại Las Vegas, ba nhà nghiên cứu Karsten Nohl, Sascha KriBler và Jakob Lell đã thông báo về lỗ hổng bảo mật trên một số thiết bị có chức năng lưu trữ USB (gọi tắt là thiết bị USB) và đặt tên là "BadUSB", nhưng chưa tiết lộ thông tin chi tiết về kỹ thuật và phương pháp thực hiện tấn công. Lỗ hổng này cho phép tin tặc cài đặt mã độc vào phần mềm điều khiển (firmware) của các thiết bị USB để từ đó có thể xâm nhập vào các máy tính kết nối với các thiết bị lưu trữ đó. Do mã độc nằm trong phần mềm điều khiển nên rất khó bị phát hiện và xử lý bằng các công cụ chống mã độc thông thường.

Trong hội nghị DerbyCon diễn ra cuối tháng 9/2014, một nhóm nghiên cứu an toàn thông tin khác (gồm Adam Caudill và Brandon Wilson) đã công bố kỹ thuật gài các mã độc vào firmware của một thiết bị USB sử dụng chip điều khiển "Phison PS2251-03 (2303) controller" và chỉ ra một số thiết bị USB có sử dụng chip điều khiển này sẽ có chung lỗi là:

- Patriot 8GB Supersonic Xpress
- Kingston DataTraveler 3.0 T111 8GB
- Silicon power marvel M60 64GB
- Toshiba TransMemory-MX™ Black 16 GB
- Patriot Stellar 64 Gb Phison

Các thông tin trên cho thấy lỗi bảo mật "BadUSB" là điểm yếu nghiêm trọng vì cho phép tin tặc tự gài các loại mã độc trực tiếp tấn công máy tính kết nối đến thiết bị USB (ví dụ : ăn cắp mật khẩu, tấn công leo thang đặc quyền, mở cổng hậu, cập nhật BIOS trái phép v.v...). Lỗ hổng này là công cụ thuận lợi để tin tặc thực hiện các cuộc tấn công có chủ đích với các mục tiêu cụ thể, riêng biệt, kể cả tấn công các hệ thống máy tính không nối mạng, các hệ thống điều khiển công nghiệp (SCADA).

Với cơ chế hoạt động trên, phạm vi ảnh hưởng sẽ không chỉ bao gồm các thiết bị USB sử dụng chip điều khiển "Phison PS2251-03 (2303) controller" mà

có thể xảy ra với toàn bộ các thiết bị USB mà firmware có khả năng cập nhật, chỉnh sửa. Như vậy, điện thoại thông minh sử dụng hệ điều hành Android và cổng giao tiếp USB cũng được cho là một trong các môi trường dễ dàng để tin tặc thực hiện khai thác lỗ hổng trên.

Hiện tại, thế giới chưa công bố các biện pháp đơn giản, hữu hiệu để kiểm tra, phát hiện các thiết bị USB đã bị gài mã độc vào firmware. Biện pháp an toàn nhất hiện đang được khuyến cáo là sử dụng các loại thiết bị USB từ nhà sản xuất chân chính, không có tính năng cập nhật, sửa đổi firmware.

Trước tình hình trên, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) kính đề nghị các đơn vị, cá nhân có điều kiện cùng tham gia nghiên cứu, chia sẻ thông tin và phối hợp với VNCERT xây dựng các giải pháp phát hiện và phòng chống lỗ hổng này, để có thể khuyến cáo cho cộng đồng.

Trước mắt, đề nghị các tổ chức, cá nhân áp dụng một số biện pháp hạn chế tối đa rủi ro mất an toàn thông tin với thiết bị USB nhiễm mã độc như sau:

1. Không kết nối thiết bị USB không chắc chắn an toàn vào các máy tính quan trọng cần bảo vệ, có thể sử dụng các thiế bị ghi nhớ ngoài khác để thay thế trong trường hợp cần thiết.

2. Tránh mua và sử dụng USB trôi nổi hoặc không có nguồn gốc rõ ràng trên thị trường (ví dụ: quà tặng, v.v...)

3. Khi kết nối USB vào máy tính cần cảnh giác với các giao diện xuất hiện yêu cầu phải cung cấp tài khoản, mật khẩu truy cập hoặc các thông tin cá nhân khác.

4. Hạn chế tối đa việc cho mượn, sử dụng chung thiết bị lưu trữ USB.

5. Khi có nghi ngờ hoặc phát hiện thiết bị USB có mã độc, đề nghị Quý cơ quan, tổ chức, cá nhân thông báo, gửi cho Trung tâm VNCERT để nghiên cứu xử lý.

Địa chỉ liên hệ: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, tầng 7 tòa nhà Nam Hải LakeView, khu đô thị Vĩnh Hoàng, phường Hoàng Văn Thụ, quận Hoàng Mai, Hà Nội. Đầu mối: chuyên viên Trần Tuấn Anh, số điện thoại: 043.640.4424, địa chỉ hộp thư điện tử: ttanh@vncert.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng Nguyễn Bắc Son (để b/c);
- Thứ trưởng Nguyễn Minh Hồng (để b/c);
- Cục An toàn thông tin (để biết);
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Vũ Quốc Khánh