BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM
CÔNG NGHỆ THÔNG TIN

Số: 04 /CV-TTCNTT

V/v: Cảnh báo điểm yếu an toàn thông tin nghiêm trọng trong các bộ vi xử lý

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

Hà Nội, ngày 08 tháng 01 năm 2018

Kính gửi: .....

Ngày 03/01/2018, các chuyên gia về an toàn thông tin của Google công bố một nhóm gồm 03 điểm yếu an toàn thông tin trong các bộ vi xử lý cho phép bất kỳ ứng dụng nào cũng có thể truy cập vào các vùng nhớ để lấy thông tin của hệ thống và thông tin của các ứng dụng khác (thay vì chỉ được truy cập vào vùng nhớ cấp cho ứng dụng).

Các điểm yếu an toàn thông tin trên có mã lỗi quốc tế là: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754. 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, 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.

Có 2 hình thức tấn công lợi dụng điểm yếu an toàn thông tin này đang được các chuyên gia đánh giá gồm:

- Hình thức tấn công được gọi là Meltdown: theo các chuyên gia, hình thức tấn công này có thể phá vỡ cơ chế bảo vệ vùng nhớ hệ thống, giúp cho các ứng dụng truy cập được vào các vùng nhớ hệ thống để lấy các thông tin như: mật khẩu, khóa đăng nhập, các thông tin được lưu trong bộ nhớ đệm .v.v...

- Hình thức tấn công được gọi là Spectre: tương tự như Meltdown, hình thức tấn công này có thể cho phép các ứng dụng truy cập vào vị trí bất kỳ trên bộ nhớ. Hình thức tấn công này có thể khai thác trên hầu hết các bộ vi xử lý hiện đại (Intel, AMD, ARM).

Các hãng sản xuất bộ vi xử lý Intel, ADM và ARM đã có xác nhận và bắt đầu đưa ra bản vá.

Việc cập nhật bản vá có thể thực hiện thông qua bản vá của hệ điều hành, hoặc nâng cấp thiết bị phần cứng, do vậy với máy tính, thiết bị bị ảnh hưởng có thể thực hiện cập nhật bản vá khi chưa có điều kiện nâng cấp bộ vi xử lý. Hiện nay các nhà sản xuất bộ vi xử lý cũng đang phối hợp với các hãng phần mềm để đưa ra bản vá cho hệ điều hành.

Nhằm 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, Trung tâm Công nghệ thông tin khuyến nghị các quản trị viên tại các cơ quan, đơn vị và người dùng thực hiện:

- Kiểm tra và cập nhật bản vá hoặc nâng cấp các hệ điều hành để tạm thời vá các điểm yếu an toàn thông tin trên. Khuyến cáo bật chức năng tự động cập nhật bản vá trên các thiết bị để đồng thời cập nhật các điểm yếu an toàn thông tin khác ngay khi có bản vá.

- 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.

- 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.

Khi triển khai các nội dung nêu trên, trong trường hợp cần thiết, Quý Đơn vị có thể liên hệ với Trung tâm Công nghệ thông tin, số điện thoại: 024.39439060, thư điện tử phongktht@most.gov.vn để được phối hợp, hỗ trợ.

Trân trọng thông báo./.

Nơi nhận:
- Như trên;
- Lãnh đạo Bộ (để b/c);
- Lưu: TTCNTT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục

Thông tin tham khảo và thông tin về bản vá cho một số các thiết bị

(Kèm theo Công văn số 09/CV-TTCNTT ngày 08/01/2018)

1. Một số thông tin về bản vá cho các thiết bị

a) Thông tin xác nhận về các dòng vi xử lý bị ảnh hưởng

- Intel

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

- ARM

https://developer.arm.com/support/security-update

b) Thông tin bản vá trên các hệ điều hành

- Linux Kernel:

https://lkml.org/lkml/2017/12/4/709

Bản vá này đã được áp dụng để hạn chế tấn công Meltdown và một phần của Spectre. Nó sẽ ảnh hưởng tới hiệu năng của hệ thống (làm giảm từ 5-30% tùy thuộc vào các tiến trình và các loại CPU khác nhau).

- Microsoft (Windows)

Windows 10 sẽ được tự động update thông qua Windows Update.

https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892

- Google (Android, ChromeOS,...)

https://support.google.com/faqs/answer/7622138

2. Thông tin tham khảo

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memorywith-side.html