

Số: 503 /CATT-NCSC
V/v Cảnh báo lỗ hổng, điểm yếu an toàn
thông tin nghiêm trọng trong
bộ vi xử lý của Intel

Hà Nội, ngày 16 tháng 5 năm 2019

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính.

Ngày 14/5/2019, 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 04 điểm yếu an toàn thông tin trong bộ vi xử lý Intel.

04 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 ...

Các hình thức tấn công lợi dụng 04 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.

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, Cục An toàn thông tin khuyến nghị các quản trị viên tại các cơ quan, đơn vị và người dùng thực hiện:

- 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

yêu đó. Tham khảo hướng dẫn rà soát, xác định và cập nhật tại *Phụ lục kèm theo*.

- 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.

- 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 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>).

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (đề b/c);
- Thứ trưởng Nguyễn Thành Hưng (đề b/c);
- Trung tâm VNCERT;
- Lưu: VT, NCSC.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Nguyễn Huy Dũng

Phụ lục
Hướng dẫn xác định máy tính bị ảnh hưởng và cập nhật bản vá
(kèm theo Công văn số /CATT-NCSC ngày 16/5/2019)

1. Danh sách sản phẩm bị ảnh hưởng và kế hoạch cập nhật của Intel

https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

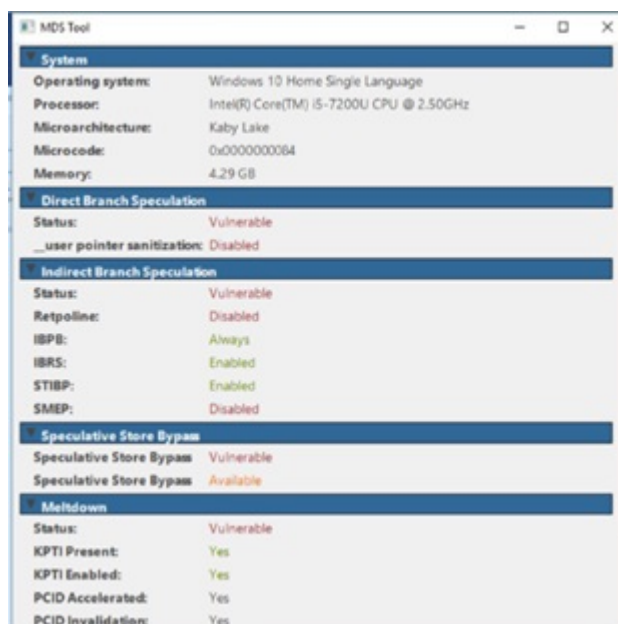
MICROCODE UPDATE GUIDANCE (1/14)

Code Name	Product Collection	Product Names	Vertical Segment	CPUID	Platform ID	OS Update Capable	Production Status	Pre-Mitigation Production MCU	New Production MCU Rev
Amber Lake Y	8 th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-8510Y, i7-8500Y Intel® Core™ Processor i5-8310Y, i5-8210Y, i5-8200Y Intel® Core™ Processor m3-8100Y	Mobile	806E9	10	Yes	Production	0x9A	0xB4
Apollo Lake	Intel® Pentium® Processor J Series Intel® Pentium® Processor N Series Intel® Celeron® Processor J Series Intel® Atom® Processor A Series Intel® Atom® Processor E3900 Series	Intel® Pentium® Processor J4205, N4200 Intel® Celeron® Processor J3355, J3455, N3350, N3450 Intel® Atom® Processor x5-A3930, x5-A394Q, x7-A3950, x7-A3960 Intel® Atom® Processor x5-E3930, x5-E3940, x7-E3950	Desktop Mobile Embedded	506C9	03	Yes	Production	0x32	0x38
Apollo Lake	Intel® Atom® Processor E3900 Series	Intel® Atom® Processor x5-E3930, x5-E3940, x7-E3950	Embedded	506CA	03	Yes	Production	0x0C	0x16
Avoton	Intel® Atom® Processor C Series	Intel® Atom® Processor C2750, C2730, C2550, C2530, C2350	Server	406D8	01	Yes	Planned	0x12A	TBA
Broadwell DE A1	Intel® Xeon® Processor D Family	Intel® Xeon® Processor D-1513N, D-1523N, D-1533N, D-1543N, D1553N	Server	50665	10	Yes	Production	0xE00000C	0xE00000D
Broadwell DE V1	Intel® Xeon® Processor D Family	Intel® Xeon® Processor D-1520, D-1540	Server	50662	10	Yes	Production	0x19	0x1A
Broadwell DE V2,V3	Intel® Xeon® Processor D Family	Intel® Xeon® Processor D-1518, D-1519, D-1521, D-1527, D-1528, D-1529, D-1531, D-1533, D-1537, D-1541, D-1548 Intel® Pentium® Processor D1507, D1508, D1509, D1517, D1519	Server	50663	10	Yes	Production	0x7000016	0x7000017
Broadwell DE Y0	Intel® Xeon® Processor D Family	Intel® Xeon® Processor D-1557, D-1559, D-1567, D-1571, D-1577, D-1581, D-1587	Server	50664	10	Yes	Production	0xF000014	0xF000015

2. Sử dụng công cụ của nhóm chuyên gia để kiểm tra trên máy

Đối với máy tính đang dùng hệ điều hành Windows

- Tải công cụ kiểm tra tại: <https://mdsattacks.com/files/mdstool-win.zip>
- Giải nén và chạy công cụ tương ứng



Đối với máy sử dụng hệ điều hành Linux

- Tải công cụ kiểm tra lỗ hổng tại: <https://mdsattacks.com/files/mdstool-linux.zip>;

- Phân quyền thực thi và chạy tập tin mdstool-linux64.bin



3. Cập nhật bản vá

- Đối với hệ điều hành Windows: Bật chương trình cập nhật bản vá tự động hoặc tải và cập nhật bản vá tại:

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013>

- Đối với hệ điều hành MacOS: tải và cập nhật tại

<https://support.apple.com/en-us/HT210107>

- Hệ điều hành Linux: tìm kiếm và cập nhật nhân cho hệ điều hành, hoặc cập nhật theo gói bản vá.

Redhat: <https://access.redhat.com/security/vulnerabilities/mds>

Ubuntu: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/MDS?_ga=2.264180484.929460546.1557968026-2003291577.1557968026

- Hệ điều hành ảo hóa của VMware

<https://www.vmware.com/security/advisories/VMSA-2019-0008.html>