

Số: 119 /TTCNTT-KTHT

Hà Nội, ngày 24 tháng 05 năm 2019

V/v Cảnh báo lỗ hổng, điểm yếu an toàn  
thông tin nghiêm trọng trong bộ vi xử lý  
của Intel

Kính gửi: Các đơn vị trực thuộc Bộ

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, Trung tâm Công nghệ thông tin khuyến nghị các quản trị viên tại các 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 yếu 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.

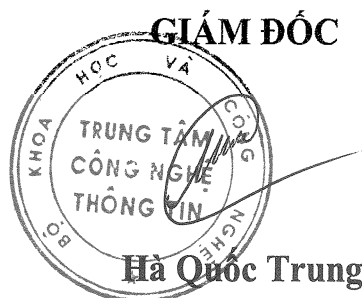
- Thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin nhằm đối phó kịp thời với các nguy cơ tấn công mạng.

Trong trường hợp cần thiết xin vui lòng liên hệ Phòng Kỹ thuật hạ tầng – Trung tâm Công nghệ thông tin, số điện thoại: 024.39439060, thư điện tử [phongktht@most.gov.vn](mailto:phongktht@most.gov.vn) để được hỗ trợ kịp thời. f

Trân trọng./.

**Nơi nhận:**

- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: TTCNTT.





## PHỤC LỤC

**Một số hình ảnh minh họa và hướng dẫn gỡ bỏ, cập nhật**  
(Kèm theo Công văn số 119 /TTCNTT-KTHT ngày 24 /05/2019 của Trung tâm Công nghệ thông tin)

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

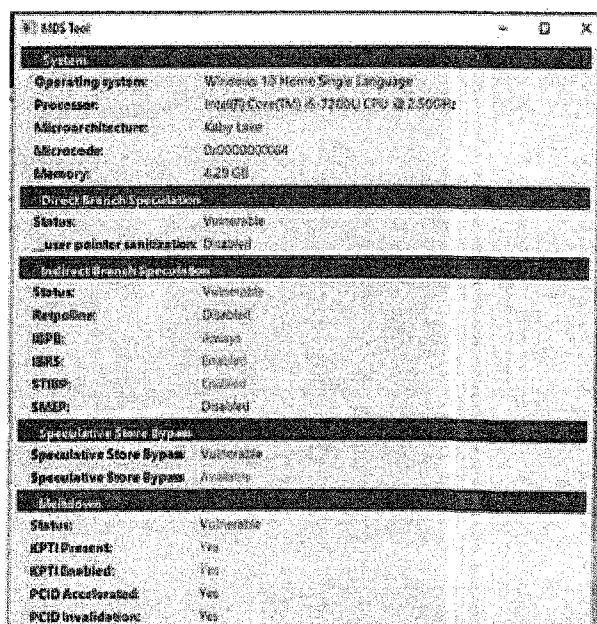
## MICROCODE UPDATE GUIDANCE (1/14)

| 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 <sup>th</sup> Generation Intel® Core® Processor Family                                                                                                                                                                       | Intel® Core® Processor i7-8510Y, i7-8500Y<br>Intel® Core® Processor i5-8110Y, i5-8100Y, i5-8100Y<br>Intel® Core® Processor m2-8100Y                                                                                    | Mobile                    | 106E9 | 10          | Yes               | Production        | 0x1A                          | 0x14                   |
| Apollo Lake     | Intel® Pentium® Processor J Series<br>Intel® Pentium® Processor N Series<br>Intel® Celeron® Processor J Series<br>Intel® Celeron® Processor N Series<br>Intel® Atom® Processor A Series<br>Intel® Atom® Processor E3900 Series | Intel® Pentium® Processor J4405, J4200<br>Intel® Celeron® Processor J3355, J3355, N3350, J3345<br>Intel® Atom® Processor x5-A3950, x5-A3940, x5-A3950, x5-A3940<br>Intel® Atom® Processor x5-E3950, x5-E3940, x5-E3950 | Desktop, Mobile, Embedded | 506C9 | 09          | Yes               | Production        | 0x12                          | 0x18                   |
| Apollo Lake     | Intel® Atom® Processor E3900 Series                                                                                                                                                                                            | Intel® Atom® Processor x5-E3950, x5-E3940, x5-E3950                                                                                                                                                                    | Embedded                  | 506CA | 03          | Yes               | Production        | 0x0C                          | 0x16                   |
| Avoton          | Intel® Atom® Processor C Series                                                                                                                                                                                                | Intel® Atom® Processor C2750, C2730, C2950, 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-1523N, D-1513N, D-1513N, D-1513N                                                                                                                                            | Server                    | 506E5 | 10          | Yes               | Production        | 0x000000C                     | 0x000000D              |
| Broadwell DE V1 | Intel® Xeon® Processor D Family                                                                                                                                                                                                | Intel® Xeon® Processor D-1516, D-1516, D-1513, D-1527, D-152A, D-1525, D-151, D-1533, D-1527, D-1541, D-1549                                                                                                           | Server                    | 506E3 | 10          | Yes               | Production        | 0x700000E                     | 0x7000007              |
| Broadwell DE V2 | Intel® Xeon® Processor D Family                                                                                                                                                                                                | Intel® Xeon® Processor D-1507, D-1507, D-1507, D-1517, D-1527, D-1541, D-1507                                                                                                                                          | Server                    | 506E4 | 10          | Yes               | Production        | 0x700000A                     | 0x7000005              |

### 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](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>