

**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: 278/CATT-TPQLGS

Hà Nội, ngày 26 tháng 5 năm 2017

V/v cảnh báo một số lỗ hổng nghiêm trọng
trong một số Chip Intel và một số
dòng máy tính HP

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 kinh tế; Tổng công ty nhà nước; Tổ chức tài
chính và ngân hàng.

HỎA-TỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG	
TỈNH GIA LAI	
ĐẾN	Số: <u>1782</u>
	Ngày: <u>31/5/2017</u>
	Chuyển: _____

Gần đây, các lỗ hổng mới trên nhiều nền tảng hệ điều hành cũng như phần mềm điều khiển (firmware) tích hợp sẵn trên các máy tính, thiết bị ngày càng được tin tặc lợi dụng để thực hiện các cuộc tấn công nguy hiểm.

Một số lỗ hổng nghiêm trọng có khả năng ảnh hưởng rộng tới các hệ thống thông tin của nhiều đơn vị như sau:

1. Lỗ hổng trong một số dòng máy sử dụng Chip Intel;
2. Lỗ hổng (keylogger) trong trình điều khiển âm thanh của một số dòng máy HP.

(Chi tiết về lỗ hổng có trong tài liệu kèm theo).

Cục An toàn thông tin đề nghị các cơ quan, tổ chức thực hiện các biện pháp bảo đảm an toàn thông tin đối với các đơn vị, cá nhân thuộc phạm vi mình quản lý như sau:

- Kiểm tra, rà soát và cập nhật bản vá của lỗ hổng bảo mật nói trên cho các máy tính, thiết bị trong hệ thống có khả năng bị ảnh hưởng;
- Rà soát và vá các lỗ hổng an toàn thông tin khác trong hệ thống;
- Tăng cường, chủ động theo dõi và có kế hoạch, biện pháp xử lý khi có lỗ hổng mới để phát hiện, ngăn chặn sớm 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 Cục An toàn thông tin, ĐT: 0439436684, thư điện tử bt_huyen@mic.gov.vn để được phối hợp, hỗ trợ.

Trân trọng./.

Nơi nhận:

- Như trên;
- Cục trưởng (để b/c);
- Lưu: VT, TĐQLGS.

**KT.CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**



Nguyễn Huy Dũng

CẢNH BÁO LỖ HỒNG TRONG MỘT SỐ DÒNG MÁY SỬ DỤNG CHIP INTEL

(Kèm theo Công văn số 273 /CATTT-TĐQLGS ngày 26/5/2017)

1. Thông tin chung

- Mức độ: Nghiêm trọng
- Mã lỗi quốc tế: CVE-2017-5689, INTEL-SA-00075
- Ảnh hưởng: Các dòng máy sử dụng công nghệ Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM) và Intel® Small Business Technology (SBT) phiên bản 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, và 11.6.

Ngày 5 tháng 5 năm 2017, nhóm các chuyên gia bảo mật Embedi đã công bố một lỗ hồng bảo mật trong các máy tính sử dụng công nghệ Intel AMT cho phép vượt qua cơ chế xác thực để chiếm quyền điều khiển hệ thống. Được biết, lỗ hồng này đã được nhóm phát hiện từ giữa tháng 3 năm 2017 trong quá trình kiểm tra các giao thức và dịch vụ mạng bên trong Intel ME firmware.

Lỗ hồng này nằm bên trong thành phần xác thực của chức năng Intel AMT Web (chức năng cho phép quản trị viên có thể quản lý các PC, máy trạm và máy chủ từ xa) được cài sẵn trên Chip của máy tính. Intel AMT/ISM lắng nghe trên một số cổng mặc định là 16992, 16993. Một số cổng liên quan khác cũng có thể được sử dụng gồm 16994, 16995, 623, 664.

Khi khai thác thành công lỗ hồng này, tin tặc hoàn toàn có thể kiểm soát máy tính nguy hiểm hơn là kiểm soát ở mức độ phần cứng, độc lập với hệ điều hành, tin tặc hoàn toàn có thể phá hủy toàn bộ dữ liệu hệ thống, xóa đi, cài lại hệ điều hành....và thực hiện bất kỳ hành vi nguy hiểm nào.

2. Khuyến nghị

Nhằm bảo đảm an toàn thông tin và phòng tránh việc tin tặc lợi dụng lỗ hồng để thực hiện những cuộc tấn công mạng nguy hiểm, Cục ATTT khuyến nghị các quản trị viên tại các cơ quan, đơn vị nhanh chóng kiểm tra và cập nhật ngay bản vá tương ứng cho các máy tính bị ảnh hưởng.

3. Một số hướng dẫn kiểm tra và cập nhật firmware.

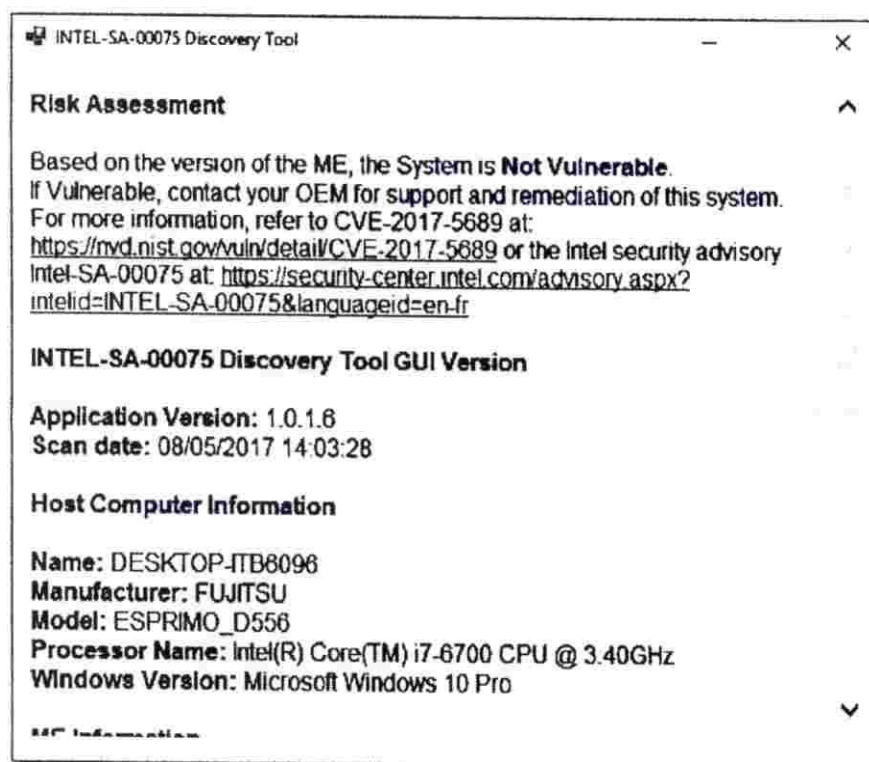
Để kiểm tra xem máy tính có bị ảnh hưởng không: có thể sử dụng một trong các cách sau:

- Kiểm tra xem có mở các cổng liên quan: sử dụng công cụ quét cổng (như nmap, netstat);
- Sử dụng công cụ do Intel phát hành;
- Kiểm tra theo từng dòng máy tính.

Kiểm tra sử dụng Công cụ của Intel:

- Windows: <https://downloadcenter.intel.com/download/26755>
- Linux (ubuntu):

<https://downloadcenter.intel.com/download/26799/INTEL-SA-00075-Linux-Detection-and-Mitigation-Tools?wapkw=intel-sa-00075>



Kiểm tra bằng công cụ của Intel trên Windows

- Kiểm tra theo danh sách các phiên bản bị ảnh hưởng của từng hãng.
 - HP Inc. - <http://www8.hp.com/us/en/intelmanageabilityissue.html>
 - HP Enterprise - <http://h22208.www2.hp.com/eginfolib/securityalerts/CVE-2017-5689-Intel/CVE-2017-5689.html>
 - Lenovo - https://support.lenovo.com/us/en/product_security/LEN-14963
 - Fujitsu - http://www.fmworld.net/globalpc/intel_firmware/
 - Dell Client - http://en.community.dell.com/techcenter/extras/m/white_papers/20443914
 - Dell EMC - http://en.community.dell.com/techcenter/extras/m/white_papers/20443937

- Acer - https://us.answers.acer.com/app/answers/detail/a_id/47162
- Asus - <https://www.asus.com/News/uztEkib4zFMHCn5r>
- Panasonic - <http://pc-dl.panasonic.co.jp/itn/info/osinfo20170512.html>
- Toshiba - <https://support.toshiba.com/sscontent?contentId=4015668>
- Intel – NUC, Compute Stick and Desktop Boards

(Theo dõi và cập nhật trên trang của Intel tại địa chỉ: <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>

Để cập nhật bản vá:

- Khuyến nghị nên theo hướng dẫn của từng dòng máy,
- Trong trường hợp chưa có thì áp dụng các biện pháp theo hướng dẫn của Intel tại <https://downloadcenter.intel.com/download/26754> (ở mức Hệ điều hành và mức mạng).

4. Tham khảo

<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>
<https://www.embedi.com/files/white-papers/Silent-Bob-is-Silent.pdf>
<https://newsroom.intel.com/news/important-security-information-intel-manageability-firmware/>