UBND TỈNH THÁI BÌNH
SỞ Y TẾ

Số: 417 /SYT-KHTC

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

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

Thái Bình, ngày 12 tháng 6 năm 2017

Kính gửi: Các đơn vị trực thuộc Sở Y tế.

Thực hiện Công văn số 225/CNTT-CSHT ngày 12/6/2017 của Cục Công nghệ thông tin - Bộ Y tế, Công văn số 273/CATTT-TĐQLGS ngày 26/5/217 của Cục an toàn thông tin – Bộ Thông tin và truyền thông về việc cảnh báo một số lỗ hổng nghiêm trọng trong một số chip Intel và một số dòng máy tính HP. Để đảm bảo an toàn thông tin trong ngành, Sở Y tế yêu cầu các đơn vị thực hiện một số nội dung sau:

1. Chỉ đạo phòng hoặc tổ công nghệ thông tin của đơn vị kiểm tra rà soát và cập nhật bản vá của lỗ hổng bảo mật như: Lỗ hổng trong một số dòng máy tính sử dụng Chip Intel; lỗ hổng (keylogger) trong trình điều khiển âm thanh của một số dòng máy HP (Chi tiết về lỗ hổng trong tài liệu gửi kèm).

2. Rà soát và vá các lỗ hổng an toàn thông tin khác trong hệ thống.

3. 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.

Trong quá trình thực hiện nếu có vướng mắc đề nghị thông tin về Sở Y tế để phối hợp xử lý, giải quyết./.

Nơi nhận:
- Như trên;
- GĐ, các PGĐ;
- Lưu: VP, KHTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
TỈNH THÁI BÌNH

Trần Quang Hải

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

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 hổng 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 hổng 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 hổng 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 gồm16994, 16995, 623, 664.

Khi khai thác thành công lỗ hổng 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 huỷ toàn bộ dữ liệu hệ thống, xoá 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 hổng 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.

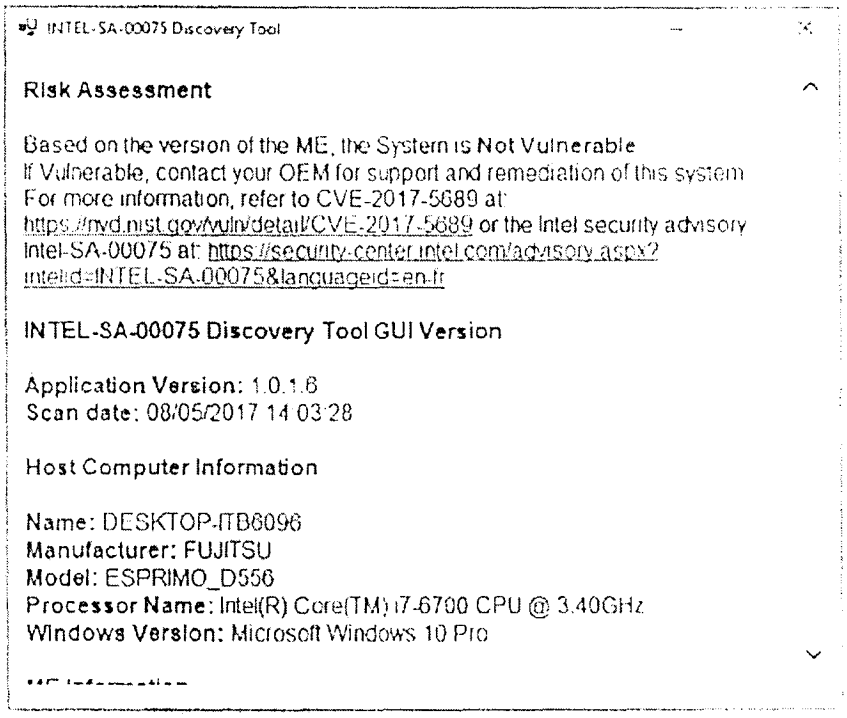
Để kiểm tra xem máy tính có bị ảnh hưởng không: có thể sử dụng một trong các cách sau:

- 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.hpe.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/

CẢNH BÁO KEYLOGGER CÀI ĐẶT SẴN TRONG MỘT SỐ DÒNG MÁY HP

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

1. Thông tin và lỗ hổng.

- Mức độ: Cao
- Mã lỗi quốc tế: CVE-2017-8360
- Ảnh hưởng: một số dòng máy HP sử dụng trình điều khiển âm thanh Conexant (tham chiếu mục 3).

Trong quá trình nghiên cứu về nhóm chuyên gia Modzero đến từ Thuỵ sĩ đã phát trình điều khiển âm thanh trong một số dòng máy HP có tích hợp sẵn chức năng ghi lại tất cả các thao tác của bàn phím. Thông thường đây là chức năng tin tặc sử dụng để ăn trộm thông tin nhạy cảm mà người dùng nhập vào từ bàn phím như tài khoản email, tài khoản ngân hàng, thông tin thẻ thanh toán....

Vị trí trình điều khiển

C:\Windows\System32\MicTray64.exe

C:\Windows\System32\MicTray.exe

Thông tin ghi vào trong file log ở C:\Users\Public\MicTray.log. Bất kỳ tiến trình nào chạy trên hệ thống cùng phiên đăng nhập của người dùng đều có quyền truy cập vào các file này. Do vậy việc thu thập những thông tin nhạy cảm này là rất dễ dàng.

Ngày 19/5 tập đoàn HP cũng đã xác nhận và đưa ra bản vá cho các dòng máy bị ảnh hưởng.

2. Khuyến nghị

- Kiểm tra loại bỏ trình điều khiển bị ảnh hưởng trên máy, xoá các file thực thi và file log nếu vẫn tồn tại trên hệ thống.
- Theo dõi và cập nhật bản vá mới cho trình điều khiển tại

https://support.hp.com/us-en/product/hp-probook-430-g3-notebook-pc/7834547/document/c05519670/

3. Danh sách dòng máy bị ảnh hưởng

HP EliteBook 820 G3 Notebook PC
HP EliteBook 828 G3 Notebook PC
HP EliteBook 840 G3 Notebook PC
HP EliteBook 848 G3 Notebook PC
HP EliteBook 850 G3 Notebook PC
HP ProBook 640 G2 Notebook PC

HP ProBook 650 G2 Notebook PC
HP ProBook 645 G2 Notebook PC
HP ProBook 655 G2 Notebook PC
HP ProBook 450 G3 Notebook PC
HP ProBook 430 G3 Notebook PC
HP ProBook 440 G3 Notebook PC
HP ProBook 446 G3 Notebook PC
HP ProBook 470 G3 Notebook PC
HP ProBook 455 G3 Notebook PC
HP EliteBook 725 G3 Notebook PC
HP EliteBook 745 G3 Notebook PC
HP EliteBook 755 G3 Notebook PC
HP EliteBook 1030 G1 Notebook PC
HP ZBook 15u G3 Mobile Workstation
HP Elite x2 1012 G1 Tablet
HP Elite x2 1012 G1 with Travel Keyboard
HP Elite x2 1012 G1 Advanced Keyboard
HP EliteBook Folio 1040 G3 Notebook PC
HP ZBook 17 G3 Mobile Workstation
HP ZBook 15 G3 Mobile Workstation
HP ZBook Studio G3 Mobile Workstation
HP EliteBook Folio G1 Notebook PC

Hệ điều hành

Microsoft Windows 10 32
Microsoft Windows 10 64
Microsoft Windows 10 IOT Enterprise 32-Bit (x86)
Microsoft Windows 10 IOT Enterprise 64-Bit (x86)
Microsoft Windows 7 Enterprise 32 Edition
Microsoft Windows 7 Enterprise 64 Edition
Microsoft Windows 7 Home Basic 32 Edition
Microsoft Windows 7 Home Basic 64 Edition
Microsoft Windows 7 Home Premium 32 Edition
Microsoft Windows 7 Home Premium 64 Edition
Microsoft Windows 7 Professional 32 Edition
Microsoft Windows 7 Professional 64 Edition
Microsoft Windows 7 Starter 32 Edition
Microsoft Windows 7 Ultimate 32 Edition
Microsoft Windows 7 Ultimate 64 Edition
Microsoft Windows Embedded Standard 7 32
Microsoft Windows Embedded Standard 7E 32-Bit

4. Tham khảo:

https://www.modzero.ch/advisories/MZ-17-01-Conexant-Keylogger.txt
https://support.hp.com/us-en/product/hp-probook-430-g3-notebook-pc/7834547/document/c05519670/