Người ký: Sở Tài nguyên và Môi trường
Email: stnmt@hungyen.gov.vn
Cơ quan: Tỉnh Hưng Yên
Thời gian ký: 13.06.2017 18:24:38 +07:00

UBND TỈNH HƯNG YÊN
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 77/STNMT- CNTT
V/v cảnh báo và thực hiện các biện pháp đảm bảo an toàn an ninh thông tin, xử lý lỗ hổng nghiêm trọng trong một số Chip Intel, máy tính HP

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

Hưng Yên, ngày 12 tháng 6 năm 2017

Kính gửi: Các phòng, đơn vị thuộc sở

Thực hiện Kế hoạch 146/KH-UBND của UBND tỉnh ngày 31/5/2017 về việc tiếp tục thực hiện Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban bí thư Trung ương Đảng về tăng cường công tác đảm bảo an toàn thông tin mạng; Công văn 1252/UBND- NC của UBND tỉnh ngày 30/5/2017 về việc Quản lý, thiết lập, đảm bảo hoạt động các trang thông tin điện tử; đảm bảo an ninh an toàn thông tin, bảo vệ bí mật nhà nước, phòng ngừa ngăn chặn mã độc; Công văn số 320/STTTT-CNTT của Sở TT&TT ngày 30/5/2017 về việc cảnh báo lỗ hổng nghiêm trọng trong một số dòng Chip Intel và máy tính HP.

Hiện nay, công tác đảm bảo an toàn an ninh thông tin đối với máy tính cá nhân, tổ chức đặc biệt là đối với các cơ quan tổ chức nhà nước ngày càng trở lên quan trọng và cấp bách. Trong thời gian vừa qua đã xảy ra rất nhiều vụ việc liên quan đến mất an toàn an ninh thông tin như việc tin tặc tấn công bằng sử dụng mã độc WannaCry (*tấn công hơn 100 quốc gia trong đó có Việt Nam*), gần đây nhất là lỗi lỗ hổng bảo mật của Chip Intel và lỗ hổng (keyloger) của dòng máy tính HP. Đây là lỗ hổng nghiêm trọng có khả năng ảnh hưởng rộng đến hệ thống thông tin của nhiều đơn vị, khi khai thác thành công lỗ hổng này, tin tặc hoàn toàn có thể kiểm soát máy tinh nguy hiểm hơn là kiểm soát ở mức độ phần cứng, độc lập với hệ điều hành như: *Xóa dữ liệu máy tính, xóa đi và cài lại hệ điều hành, ghi lại các thao tác trên bàn phím của nạn nhân, .. và có thể thực hiện bất kì các hành vi nguy hiểm nào.*

Để phòng ngừa và thực hiện các biện pháp đảm bảo an toàn thông tin với các máy tính, thiết bị công nghệ thông tin trong phòng, đơn vị của mình, lựa chọn mua sắm máy tính, thiết bị đảm bảo an toàn. Sở Tài nguyên và Môi trường yêu cầu các

phòng, đơn vị triển khai ngay một số biện pháp nhằm đảm bảo an toàn, an ninh thông tin của phòng, đơn vị, cá nhân như sau:

1. Tiếp tục thực hiện các biện pháp đảm bảo an toàn an ninh thông tin của phòng, đơn vị theo Công văn số 569/STNMT-CNTT của Sở Tài nguyên và môi trường ngày 18/5/2017 về việc thực hiện các biện pháp xử lý mã độc WannaCry trong hệ thống mạng.

2. Tiến hành rà soát, cập nhật bản vá lỗ hổng bảo mật nói trên cho các dòng máy tính, thiết bị trong hệ thống có khả năng bị ảnh hưởng *(theo hướng dẫn đính kèm)*

3. Lãnh đạo các phòng, đơn vị cử cán bộ có đủ năng lực phụ trách về an toàn và an ninh, chịu trách nhiệm đảm bảo an ninh và an toàn hệ thống thông tin của phòng, đơn vị mình quản lý.

4. Trung tâm Công nghệ thông tin tài nguyên môi trường có trách nhiệm hướng dẫn các quy định, biện pháp đảm bảo an toàn an ninh thông tin cho các phòng, đơn vị. Kiểm tra, rà soát hệ thống mạng, Cổng thông tin điện tử của Sở, đảm bảo tính sẵn sàng thông tin và hệ thống thông tin khi xảy ra sự cố mất an toàn thông tin, an ninh mạng. Kịp thời phối hợp với cơ quan chức năng (Công an tỉnh, Sở thông tin và truyền thông) ngăn chặn, khắc phục khi phát hiện có dấu hiệu mất an toàn thông tin hoặc bị tấn công.

Yêu cầu các phòng, đơn vị khẩn trương thực hiện ngay các biện pháp nêu trên. Trong quá trình triển khai, nếu có vướng mắc đề nghị liên hệ với Trung tâm Công nghệ thông tin - Sở Tài nguyên và Môi trường, điện thoại: 02213.551.337 ; thư điện tử cntt.tnmt@hungyen.gov.vn; hoặc Đ/c Vũ Quốc Trịnh – Điện thoại: 0936.58.28.26 để được hướng dẫn, giải đáp./.

Nơi nhận:
- UBND tỉnh(thay b/c)
- Lãnh đạo Sở;
- Sở Thông tin và Truyền thông(để b/c)
- Như kính gửi;
- Lưu: VP, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH HƯNG YÊN

Trần Đăng Anh

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 279/CATTT-TĐQLGS
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

Hà Nội, ngày 26 tháng 5 năm 2017

SỞ THÔNG TIN VÀ TRUYỀN THÔNG HƯNG YÊN
ĐẾN Số: 1133 Kính gửi:
Ngày 30/5/2017
Chuyển: cơ

- 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

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, TDQLGS.

KT.CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

CẢNH BÁO LỖ HỔNG 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 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.

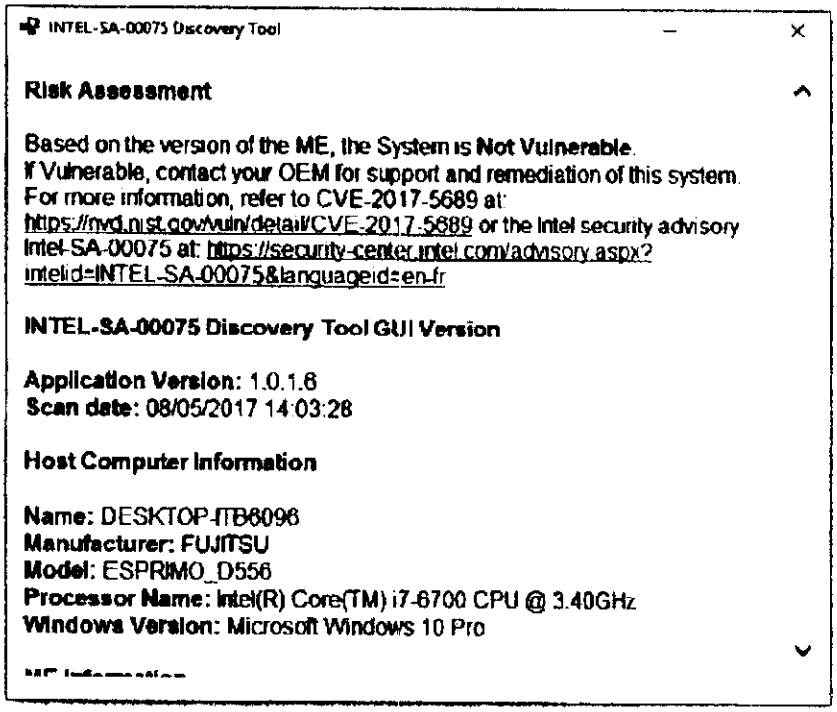
Để kiểm tra xem máy tính có bị ảnh hưởng không: có thể sử dụng một trong các cách sau:

- 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/