

UBND TỈNH QUẢNG BÌNH  
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 438/STTTT-CNTT

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

Quảng Bình, ngày 07 tháng 6 năm 2017

- Kính gửi:
- Văn phòng Tỉnh ủy, Văn phòng HĐND tỉnh;
  - Các sở, ban, ngành cấp tỉnh;
  - Các huyện, thành, thị ủy;
  - UBND các huyện, thị xã, thành phố;
  - Các cơ quan Trung ương trên địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận được Công văn số 273/CATTT-TĐQLGS ngày 26/05/2017 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. Theo đó, Cục An toàn thông tin cho biết: 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 cơ quan, đơn vị như:

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

Để đảm bảo an toàn thông tin mạng, phòng ngừa sự cố mất an toàn thông tin có thể xảy ra, Sở Thông tin và Truyền thông đề nghị thủ trưởng các cơ quan, đơn vị chỉ đạo 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, vá các lỗ hổng an toàn thông tin khác trong hệ thống và tăng cường chủ động theo dõi, có kế hoạch, biện pháp xử lý khi có lỗ hổng mới để phát hiện, ngăn chặn sớm các nguy cơ tấn công mạng; thường xuyên cập nhật vào chuyên mục **An toàn thông tin** trên Trang thông tin điện tử của Sở Thông tin và Truyền thông để nắm bắt thông tin (có Phụ lục cảnh báo, khuyến nghị và hướng dẫn xử lý kèm theo).

Quá trình thực hiện, nếu có vướng mắc, xin liên hệ về Trung tâm CNTT&TT, Sở Thông tin và Truyền thông (điện thoại 0232.3856696) để phối hợp xử lý.

Trân trọng./.

**Nơi nhận**

- Như trên;
- Cục An toàn thông tin { báo cáo }
- Trung tâm CNTT { để thực hiện };
- Lưu: VT, CNTT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Nguyễn Phi Khanh**

## **Phụ lục**

*(Kèm theo Công văn số: 438/STTTT-CNTT ngày 07 tháng 6 năm 2017)*

# **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 gồm 16994, 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 phân cứng, độc lập với hệ điều hành, tin tặc hoàn toàn có thể phá hủy 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, 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://downloadcenterintelxom/download/26799/INTEL-SA-00075-Linux-Detection-and-Mitigation-Tools?wapkw=intel-sa-00075>

INTEL-SA-00075 Discovwy Tool

-

Risk Assessment

Based on the version of the ME, the System is Not Vulnerable If Vulnerable, contact your OEM for support and remediation of this system For more information, refer to CVE-2017-5689 at <http://www.nist.gov/vuln/vuln-detail/cve-2017-5689> or the Intel security advisory Intel-SA-00075 at: <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&lanmiaueid=en-fr>

INTEL-SA-00075 Discovery Tool GUI Version

Application Version: 1.0.1.6 Scan date: 08/05/2017 14 03 28

Host Computer Information

Name: DESKTOP-ITD6096 Manufacturer: FUJITSU Model: ESPRIMO\_D556

Processor Name: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz Windows Version:

Microsoft Windows 10 Pro

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](https://support.lenovo.com/us/en/product_security/LEN-14963)

• Fujitsu - [http://www.fmworld.net/globalpc/intel\\_firmware/](http://www.fmworld.net/globalpc/intel_firmware/)

• Dell Client -

[http://en.community.dell.com/techcenter/extras/rn/white\\_papers/20443914](http://en.community.dell.com/techcenter/extras/rn/white_papers/20443914)

• Dell EMC-

[http://en.community.dell.com/techcenter/extras/rn/white\\_papers/20443937](http://en.community.dell.com/techcenter/extras/rn/white_papers/20443937)

• Acer - [https://us.answers.acer.com/app/answers/detail/a\\_id/47162](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/sscontent7contentIcN4015668>

• Intel - NUC, Compute Stick and Desktop Boards

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&lanmiaueid=en-fr>

<https://www.einbedi.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

## 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.

Trong quá trình nghiên cứu về nhóm chuyên gia Modzero đến từ Thụy sĩ đã phát hiện 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, xóa 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/>