UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 1168/SGDĐT-VP
V/v 04 lỗ hổng mới trong BIOS của máy tính, thiết bị DELL

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

Hưng Yên, ngày 05 tháng 7 năm 2021

Gửi đc Thuỷ, Kiểm chỉ đạo các đơn vị trường học rà soát, tổ hợp BC

Kính gửi:
- Các đơn vị giáo dục trực thuộc;
- Phòng GDĐT các huyện/thị xã/thành phố;
- Trung tâm GDNN – GDTX các huyện/thị xã/thành phố;

Căn cứ Công văn số 670/STTT-BCVTCNTT ngày 02/7/2021 của Sở Thông tin và Truyền thông Hưng Yên v/v 04 lỗ hổng mới trong BIOS của máy tính, thiết bị DELL. Theo thông báo của Cục an toàn thông tin v/v 04 lỗ hổng mới trong BIOS của máy tính, thiết bị DELL (CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574) có thể kết nối với nhau trong các chiến dịch tấn công có chủ đích để tấn công, kiểm soát máy tính, thiết bị của người dung, từ đó tấn công sâu vào các hệ thống thông tin quan trọng khác.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của đơn vị, góp phần bảo đảm an toàn không gian mạng Việt Nam, đề nghị đơn vị, trường học chỉ đạo bộ phận chuyên môn thực hiện ra soát, khắc phục những lỗ hổng trên theo khuyến nghị sau:

1. Kiểm tra, rà soát máy tính, thiết bị có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật mới (CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574) để có phương án xử lý, khắc phục kịp thời. Cập nhật bản vá tương ứng theo phát hành của hãng, trong trường hợp chưa có bản vá cần có phương án để ngăn chặn việc khai thác lỗ hổng, đồng thời theo dõi thường xuyên thông tin về lỗ hổng để cập nhật ngay khi có bản vá *(tham khảo hướng dẫn kèm theo Công văn số 806/CATT-NCSC gửi kèm).*

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Đề nghị đơn vị, trường học và tổ chức thực hiện./.

Nơi nhận:
- Như trên;
- Ban Giám đốc;
- Các phòng thuộc Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XH CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HƯNG YÊN

Đỗ Tiến Hùng

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: 806 /CATTT-NCSC
V/v 04 lỗ hổng mới trong BIOS của máy tính, thiết bị Dell

Hà Nội, ngày 29 tháng 06 năm 2021

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, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 24/6/2021, qua công tác giám sát trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã ghi nhận **04** điểm yếu, lỗ hổng bảo mật mới **(CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574)** trong tính năng BIOSConnect và HTTPS Boot (tính năng, công cụ có sẵn trên hầu hết các máy tính, thiết bị của hãng Dell để hỗ trợ việc cập nhật firmware và khôi phục hệ điều hành từ xa) trên BIOS của các máy tính, thiết bị hãng Dell.

Theo đánh giá sơ bộ, đây là những lỗ hổng có phạm vi ảnh hưởng tương đối lớn, đến khoảng 30 triệu thiết bị tương ứng với 129 dòng máy tính xách tay, máy tính bảng và máy tính bàn. Đặc biệt 04 lỗ hổng này có thể kết hợp với nhau trong các chiến dịch tấn công có chủ đích để tấn công, kiểm soát máy tính, thiết bị của người dùng, từ đó tấn công sâu hơn vào các hệ thống thông tin quan trọng khác (thông tin chi tiết có tại phụ lục kèm theo).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát máy tính, thiết bị có khả năng bị ảnh hưởng bởi các lỗ hổng

trên để có phương án xử lý, khắc phục kịp thời. Cập nhật bản vá tương ứng theo phát hành của hãng. Trong trường hợp chưa có bản vá cần có phương án để ngăn chặn việc khai thác lỗ hổng, đồng thời theo dõi thường xuyên thông tin về lỗ hổng để cập nhật ngay khi có bản vá (tham khảo hướng dẫn kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

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

Nguyễn Thành Phúc

Phụ lục
Thông tin về các lỗ hổng bảo mật
(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

1. Thông tin về các lỗ hổng

TT	Mã lỗi	Mức độ	Mô tả
1	CVE-2021-21571	Trung bình CVSS (3.1): 5.9	Lỗ hổng trong Dell BIOSConnect và Dell HTTPS Boot cho phép giả mạo chứng thư số.
2	CVE-2021-21572, CVE-2021-21573, CVE-2021-21574	Cao CVSS (3.1): 7.2	Lỗi tràn bộ đệm cho phép vượt qua các cơ chế kiểm soát để thực thi các đoạn mã độc hại với quyền người dùng quản trị. Khai thác được khi có quyền truy cập cục bộ.

2. Các sản phẩm bị ảnh hưởng

Sản phẩm ảnh hưởng	Phiên bản BIOS cần cập nhật	Supports BIOSConnect	Supports HTTP(s) Boot	Ngày phát hành (MM/DD/YYYY)
Alienware m15 R6	1.3.3	Yes	Yes	6/21/2021
ChengMing 3990	1.4.1	Yes	No	6/23/2021
ChengMing 3991	1.4.1	Yes	No	6/23/2021
Dell G15 5510	1.4.0	Yes	Yes	6/21/2021
Dell G15 5511	1.3.3	Yes	Yes	6/21/2021
Dell G3 3500	1.9.0	Yes	No	6/24/2021
Dell G5 5500	1.9.0	Yes	No	6/24/2021
Dell G7 7500	1.9.0	Yes	No	6/23/2021
Dell G7 7700	1.9.0	Yes	No	6/23/2021
Inspiron 14 5418	2.1.0 A06	Yes	Yes	6/24/2021

Inspiron 15 5518	2.1.0 A06	Yes	Yes	6/24/2021
Inspiron 15 7510	1.0.4	Yes	Yes	6/23/2021
Inspiron 3501	1.6.0	Yes	No	6/23/2021
Inspiron 3880	1.4.1	Yes	No	6/23/2021
Inspiron 3881	1.4.1	Yes	No	6/23/2021
Inspiron 3891	1.0.11	Yes	Yes	6/24/2021
Inspiron 5300	1.7.1	Yes	No	6/23/2021
Inspiron 5301	1.8.1	Yes	No	6/23/2021
Inspiron 5310	2.1.0	Yes	Yes	6/23/2021
Inspiron 5400 2n1	1.7.0	Yes	No	6/23/2021
Inspiron 5400 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 5401	1.7.2	Yes	No	6/23/2021
Inspiron 5401 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 5402	1.5.1	Yes	No	6/23/2021
Inspiron 5406 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 5408	1.7.2	Yes	No	6/23/2021
Inspiron 5409	1.5.1	Yes	No	6/23/2021
Inspiron 5410 2-in-1	2.1.0	Yes	Yes	6/23/2021
Inspiron 5501	1.7.2	Yes	No	6/23/2021
Inspiron 5502	1.5.1	Yes	No	6/23/2021
Inspiron 5508	1.7.2	Yes	No	6/23/2021
Inspiron 5509	1.5.1	Yes	No	6/23/2021
Inspiron 7300	1.8.1	Yes	No	6/23/2021
Inspiron 7300 2n1	1.3.0	Yes	No	6/23/2021
Inspiron 7306 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 7400	1.8.1	Yes	No	6/23/2021
Inspiron 7500	1.8.0	Yes	No	6/23/2021
Inspiron 7500 2n1 - Black	1.3.0	Yes	No	6/23/2021
Inspiron 7500 2n1 - Silver	1.3.0	Yes	No	6/23/2021
Inspiron 7501	1.8.0	Yes	No	6/23/2021

Inspiron 7506 2n1	1.5.1	Yes	No	6/23/2021
Inspiron 7610	1.0.4	Yes	Yes	6/23/2021
Inspiron 7700 AIO	1.4.0	Yes	No	6/23/2021
Inspiron 7706 2n1	1.5.1	Yes	No	6/23/2021
Latitude 3120	1.1.0	Yes	No	6/23/2021
Latitude 3320	1.4.0	Yes	Yes	6/23/2021
Latitude 3410	1.9.0	Yes	No	6/23/2021
Latitude 3420	1.8.0	Yes	No	6/23/2021
Latitude 3510	1.9.0	Yes	No	6/23/2021
Latitude 3520	1.8.0	Yes	No	6/23/2021
Latitude 5310	1.7.0	Yes	No	6/24/2021
Latitude 5310 2 in 1	1.7.0	Yes	No	6/24/2021
Latitude 5320	1.7.1	Yes	Yes	6/21/2021
Latitude 5320 2-in-1	1.7.1	Yes	Yes	6/21/2021
Latitude 5410	1.6.0	Yes	No	6/23/2021
Latitude 5411	1.6.0	Yes	No	6/23/2021
Latitude 5420	1.8.0	Yes	Yes	6/22/2021
Latitude 5510	1.6.0	Yes	No	6/23/2021
Latitude 5511	1.6.0	Yes	No	6/23/2021
Latitude 5520	1.7.1	Yes	Yes	6/21/2021
Latitude 5521	1.3.0 A03	Yes	Yes	6/22/2021
Latitude 7210 2-in-1	1.7.0	Yes	No	6/23/2021
Latitude 7310	1.7.0	Yes	No	6/23/2021
Latitude 7320	1.7.1	Yes	Yes	6/23/2021
Latitude 7320 Detachable	1.4.0 A04	Yes	Yes	6/22/2021
Latitude 7410	1.7.0	Yes	No	6/23/2021
Latitude 7420	1.7.1	Yes	Yes	6/23/2021
Latitude 7520	1.7.1	Yes	Yes	6/23/2021
Latitude 9410	1.7.0	Yes	No	6/23/2021
Latitude 9420	1.4.1	Yes	Yes	6/23/2021
Latitude 9510	1.6.0	Yes	No	6/23/2021
Latitude 9520	1.5.2	Yes	Yes	6/23/2021
Latitude 5421	1.3.0 A03	Yes	Yes	6/22/2021
OptiPlex 3080	2.1.1	Yes	No	6/23/2021

OptiPlex 3090 UFF	1.2.0	Yes	Yes	6/23/2021
OptiPlex 3280 All-in-One	1.7.0	Yes	No	6/23/2021
OptiPlex 5080	1.4.0	Yes	No	6/23/2021
OptiPlex 5090 Tower	1.1.35	Yes	Yes	6/23/2021
OptiPlex 5490 AIO	1.3.0	Yes	Yes	6/24/2021
OptiPlex 7080	1.4.0	Yes	No	6/23/2021
OptiPlex 7090 Tower	1.1.35	Yes	Yes	6/23/2021
OptiPlex 7090 UFF	1.2.0	Yes	Yes	6/23/2021
OptiPlex 7480 All-in-One	1.7.0	Yes	No	6/23/2021
OptiPlex 7490 All-in-One	1.3.0	Yes	Yes	6/24/2021
OptiPlex 7780 All-in-One	1.7.0	Yes	No	6/23/2021
Precision 17 M5750	1.8.2	Yes	No	6/9/2021
Precision 3440	1.4.0	Yes	No	6/23/2021
Precision 3450	1.1.35	Yes	Yes	6/24/2021
Precision 3550	1.6.0	Yes	No	6/23/2021
Precision 3551	1.6.0	Yes	No	6/23/2021
Precision 3560	1.7.1	Yes	Yes	6/21/2021
Precision 3561	1.3.0 A03	Yes	Yes	6/22/2021
Precision 3640	1.6.2	Yes	No	6/23/2021
Precision 3650 MT	1.2.0	Yes	Yes	6/24/2021
Precision 5550	1.8.1	Yes	No	6/23/2021
Precision 5560	1.3.2	Yes	Yes	6/23/2021
Precision 5760	1.1.3	Yes	Yes	6/16/2021
Precision 7550	1.8.0	Yes	No	6/23/2021
Precision 7560	1.1.2	Yes	Yes	6/22/2021
Precision 7750	1.8.0	Yes	No	6/23/2021
Precision 7760	1.1.2	Yes	Yes	6/22/2021
Vostro 14 5410	2.1.0 A06	Yes	Yes	6/24/2021
Vostro 15 5510	2.1.0 A06	Yes	Yes	6/24/2021
Vostro 15 7510	1.0.4	Yes	Yes	6/23/2021
Vostro 3400	1.6.0	Yes	No	6/23/2021

Vostro 3500	1.6.0	Yes	No	6/23/2021
Vostro 3501	1.6.0	Yes	No	6/23/2021
Vostro 3681	2.4.0	Yes	No	6/23/2021
Vostro 3690	1.0.11	Yes	Yes	6/24/2021
Vostro 3881	2.4.0	Yes	No	6/23/2021
Vostro 3888	2.4.0	Yes	No	6/23/2021
Vostro 3890	1.0.11	Yes	Yes	6/24/2021
Vostro 5300	1.7.1	Yes	No	6/23/2021
Vostro 5301	1.8.1	Yes	No	6/23/2021
Vostro 5310	2.1.0	Yes	Yes	6/23/2021
Vostro 5401	1.7.2	Yes	No	6/23/2021
Vostro 5402	1.5.1	Yes	No	6/23/2021
Vostro 5501	1.7.2	Yes	No	6/23/2021
Vostro 5502	1.5.1	Yes	No	6/23/2021
Vostro 5880	1.4.0	Yes	No	6/23/2021
Vostro 5890	1.0.11	Yes	Yes	6/24/2021
Vostro 7500	1.8.0	Yes	No	6/23/2021
XPS 13 9305	1.0.8	Yes	No	6/23/2021
XPS 13 2in1 9310	2.3.3	Yes	No	6/23/2021
XPS 13 9310	3.0.0	Yes	No	6/24/2021
XPS 15 9500	1.8.1	Yes	No	6/23/2021
XPS 15 9510	1.3.2	Yes	Yes	6/23/2021
XPS 17 9700	1.8.2	Yes	No	6/9/2021
XPS 17 9710	1.1.3	Yes	Yes	6/15/2021

3. Hướng dẫn khắc phục

3.1. Đối với những máy tính cập nhật bản vá BIOS

Có nhiều cách để cập nhật BIOS. Theo khuyến nghị của hãng, người dùng có thể sử dụng một trong các cách sau:

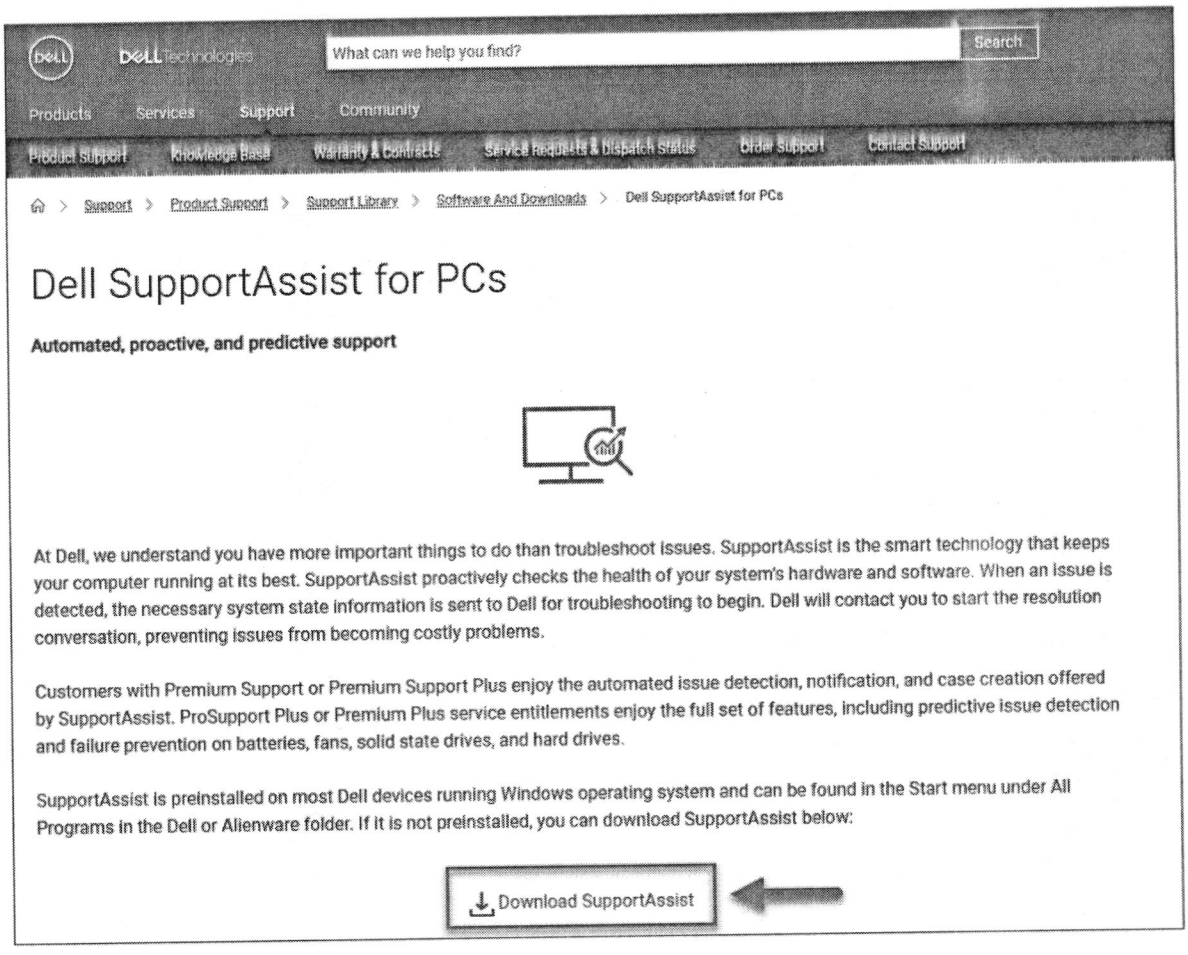
Cách 1: Cài đặt ứng dụng của Dell Notification để nhận thông báo tự động và cập nhật khi có bản vá mới.

Cách 2: Tải bản vá và cài đặt thủ công.

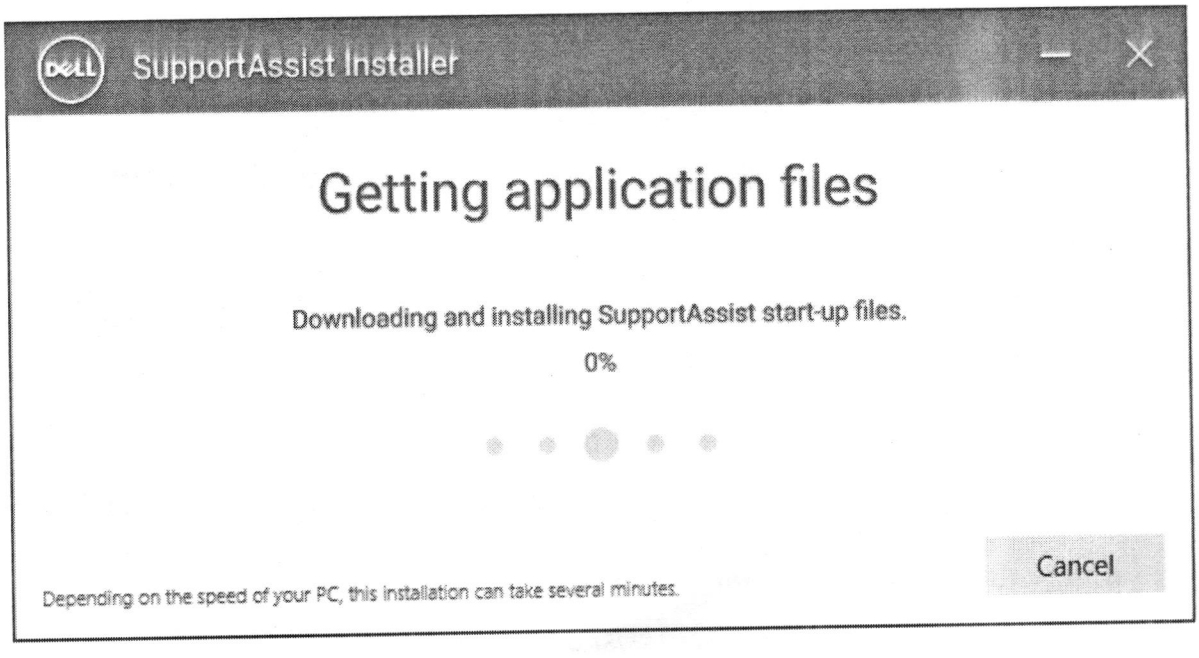
3.1.1. Cách 1: Cài đặt ứng dụng hỗ trợ của DELL để nhận thông báo cập nhật và cập nhật khi có bản vá mới.

a) Cài đặt ứng dụng SupportAssist của DELL

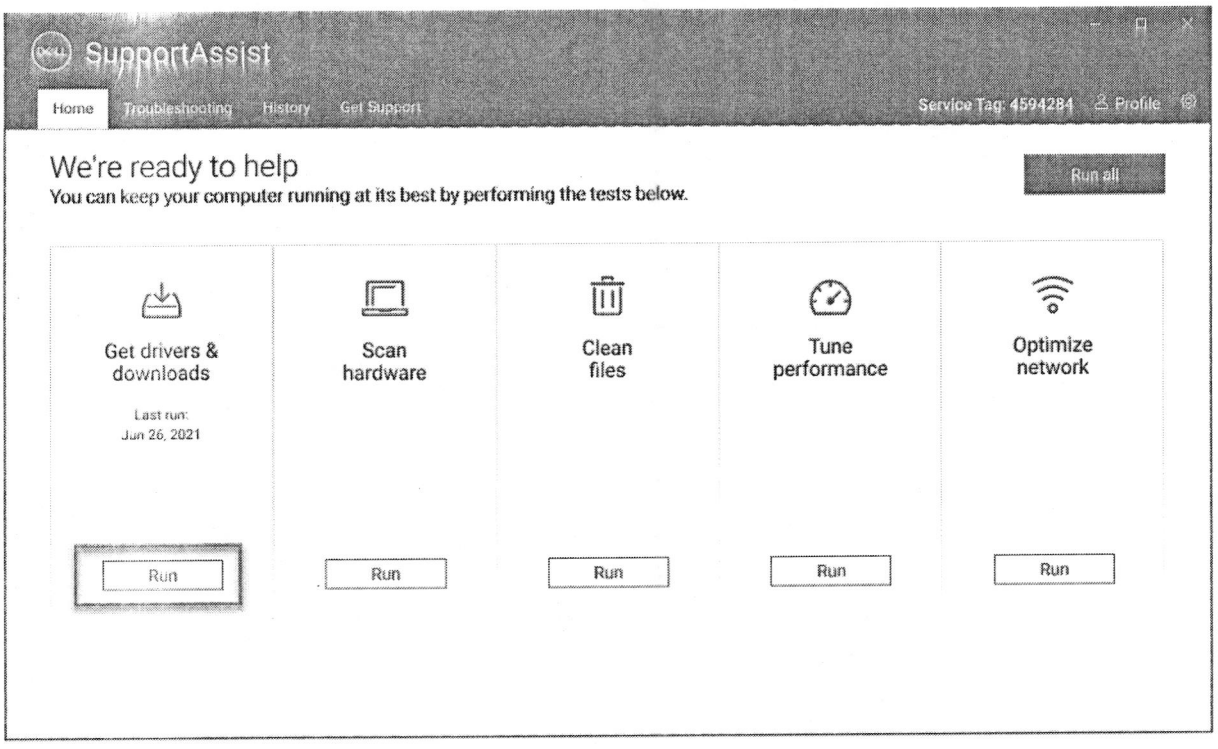
- **B1:** Truy cập vào trang: https://www.dell.com/support/contents/en-vn/article/product-support/self-support-knowledgebase/software-and-downloads/supportassist chọn ***Download SupportAssist***



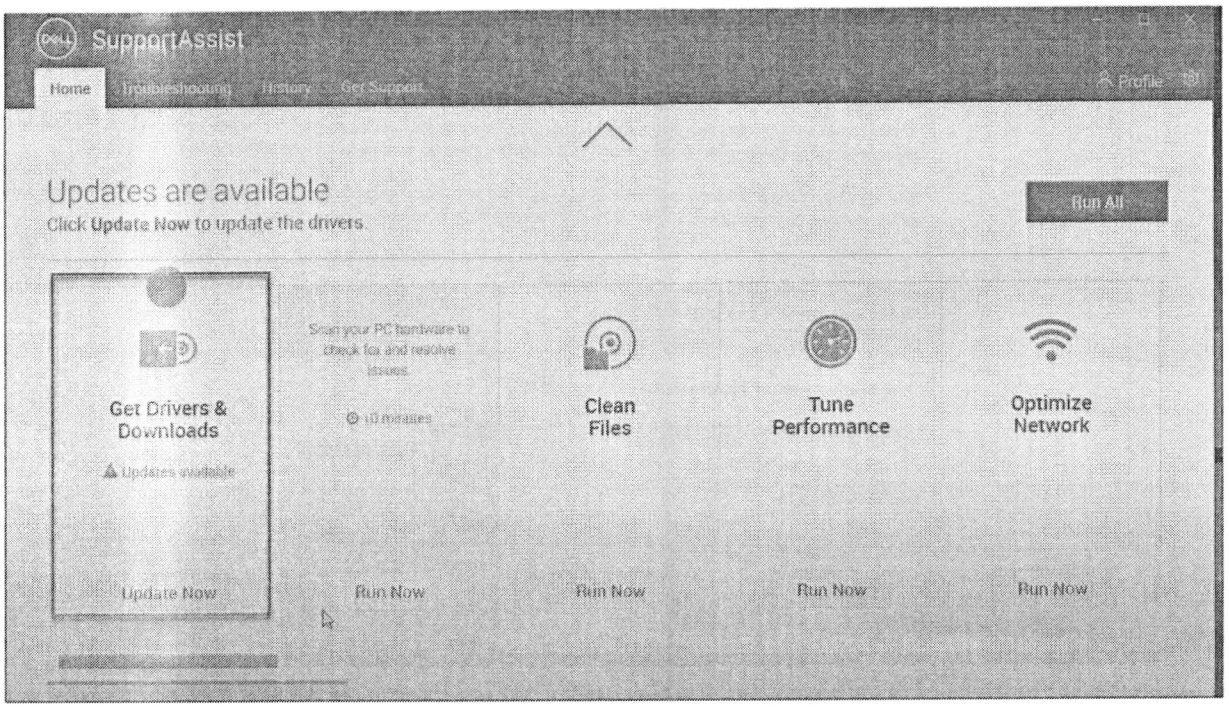
- **B2:** Cài đặt bộ cài ***SupportAssistInstaller.exe***



- **B3:** Sau khi cài đặt, vào ứng dụng ***SupportAssist.*** Tại mục ***Get driver & Downloads*** chọn ***Run*** để bắt đầu kiểm tra các bản vá, cập nhật của máy

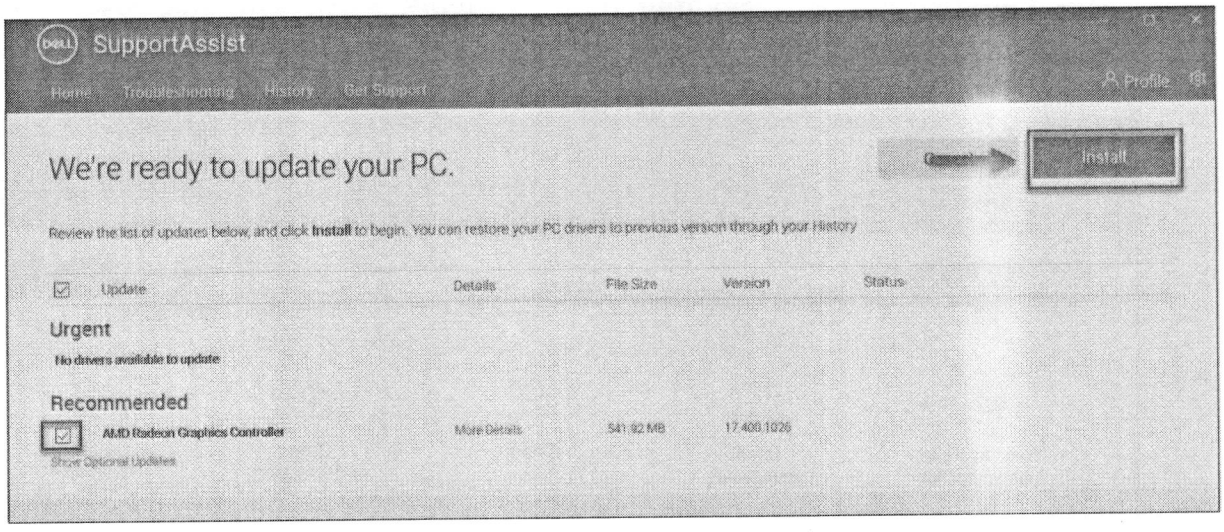


- ***B4:*** Sau khi chạy, nếu có bản cập nhật, ứng dụng sẽ hiện thông báo



+ Chọn ***Update Now*** để kiểm tra thông tin các bản cập nhật đã tải về. Chọn các bản cập nhật được cài/không được cài vào máy bằng cách tích vào ô đầu mỗi bản cập nhật

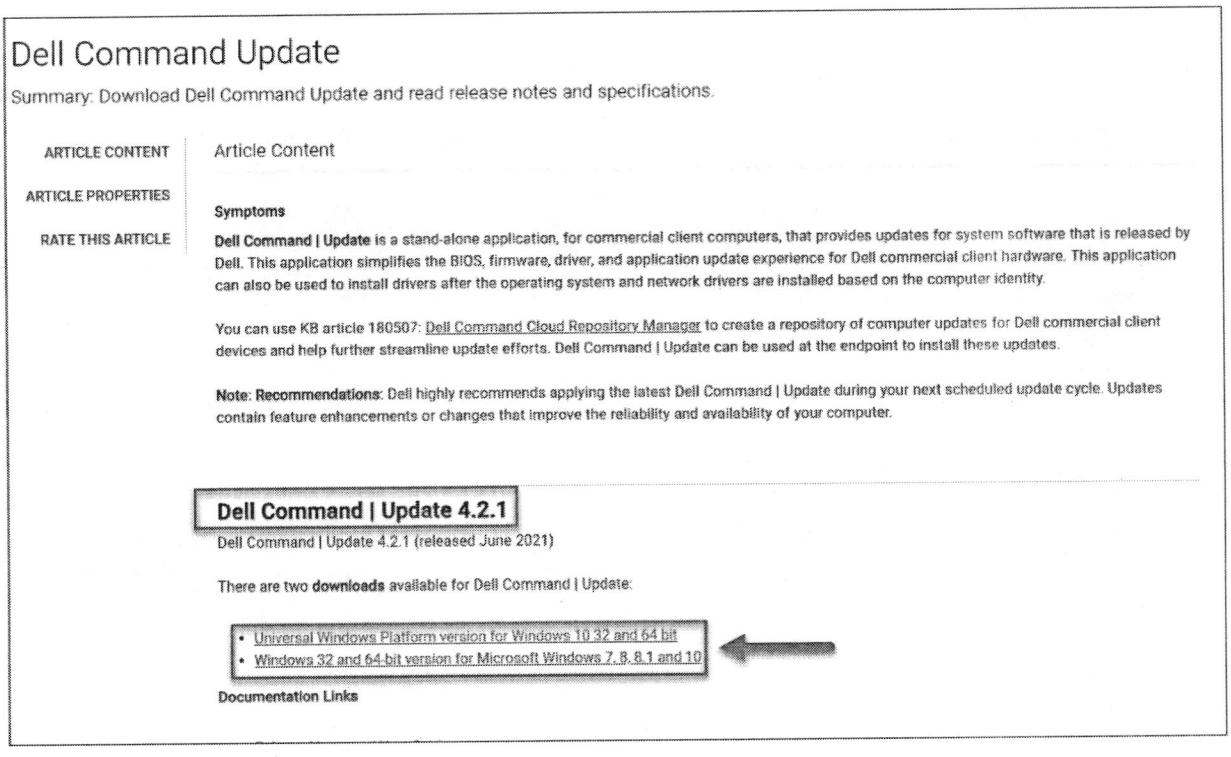
+ Chọn **Install** để bắt đầu quá trình cập nhật, khởi động lại máy nếu ứng dụng yêu cầu



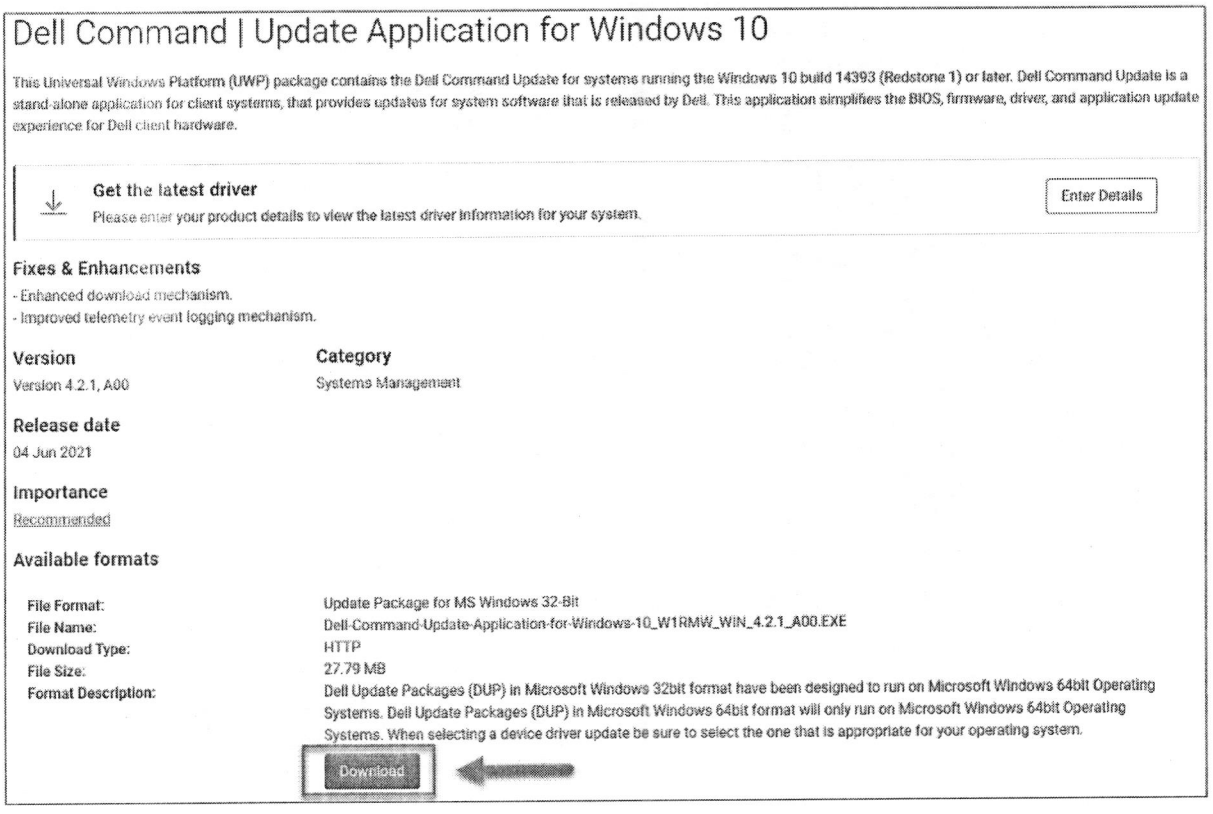
b) Cài đặt ứng dụng DELL Update

- **B1:** Truy cập trang: https://www.dell.com/support/kbdoc/en-vn/000177325/dell-command-update

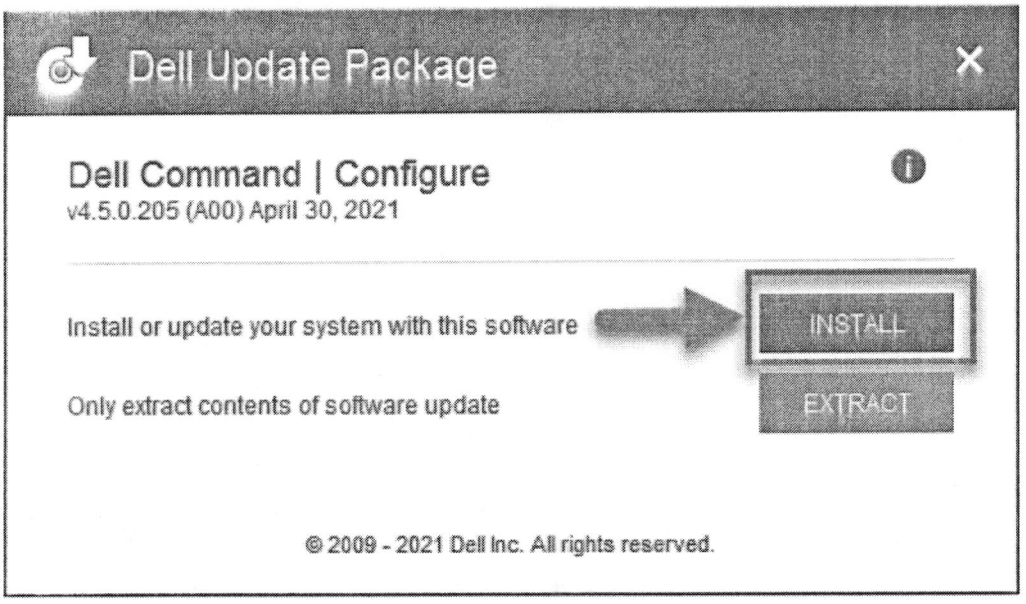
+ Chọn ***Version Dell Update*** và download ứng dụng

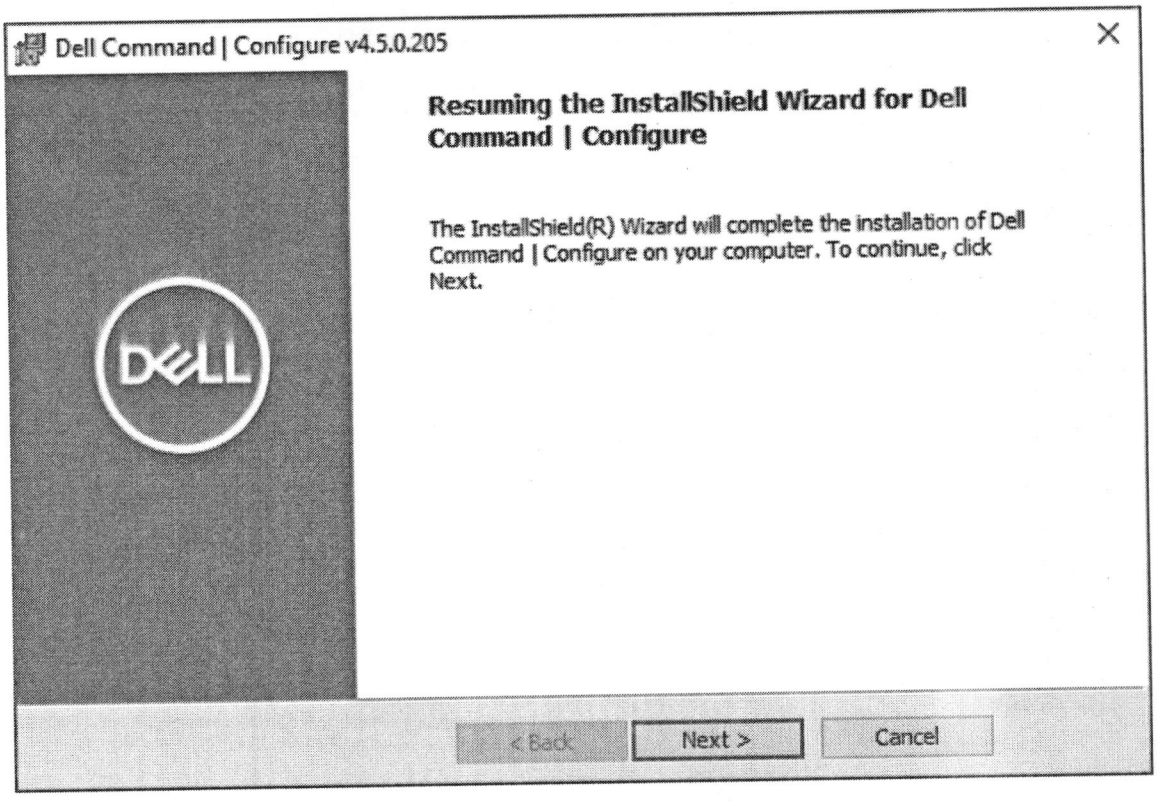


+ Chọn ***download*** tại trang vừa mở ra sau khi click vào link trên

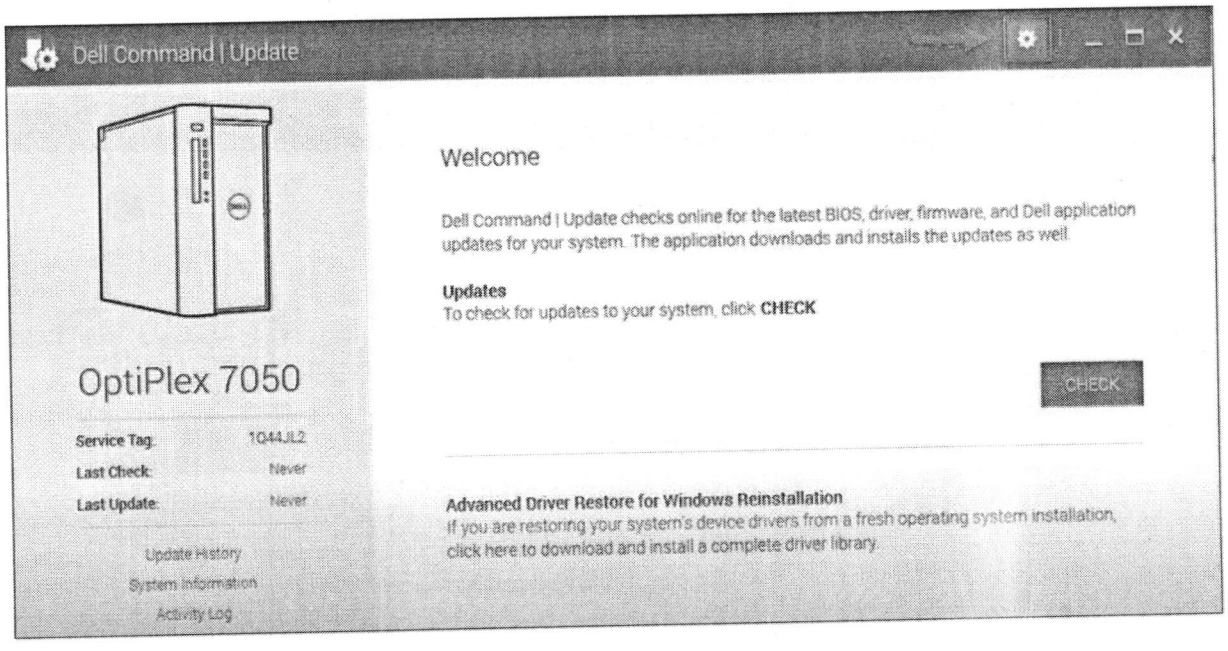


- **B2:** Cài đặt ứng dụng





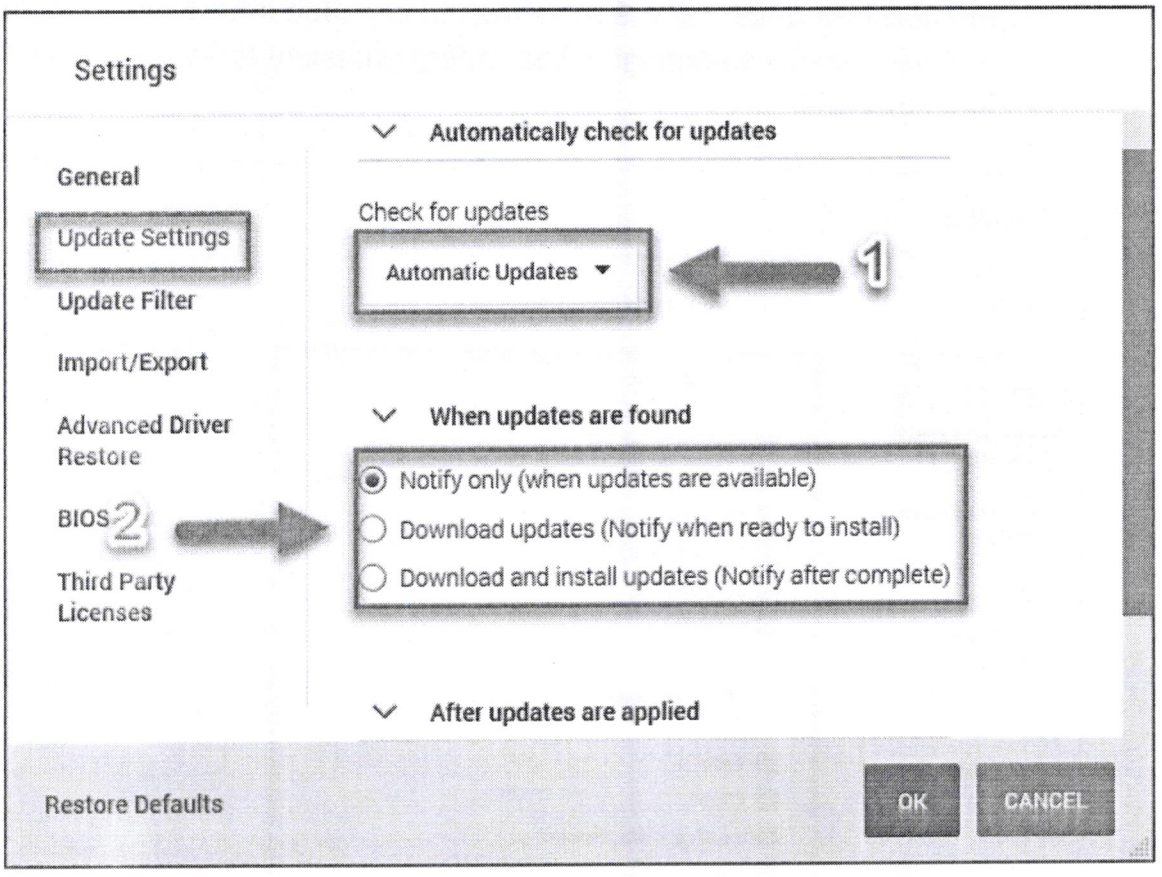
- **B3:** Sau khi cài đặt, tại ứng dụng ***Dell Command Update***, chọn ***Setting***



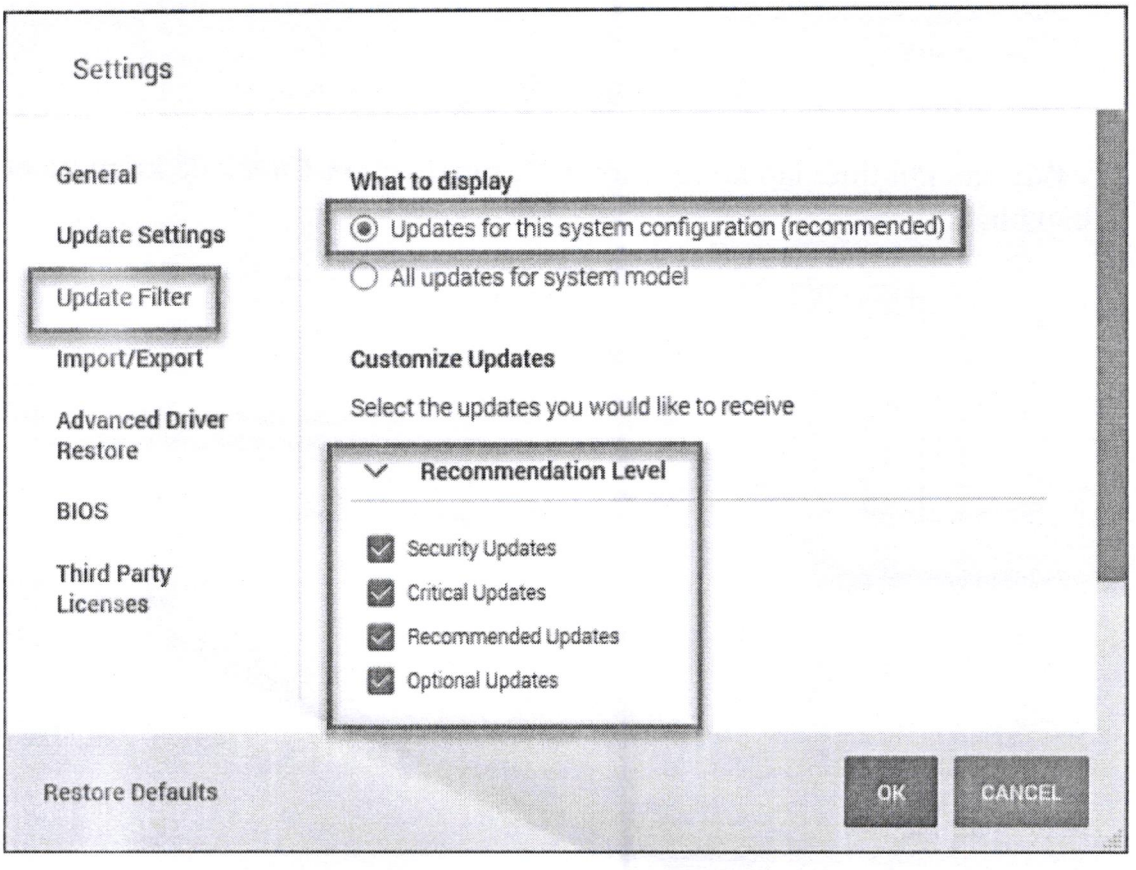
- **B4:** Tại cửa sổ ***Setting***, chọn ***Update Settings*** để thiết lập cấu hình cho việc cập nhật bản vá

+ ***Mục 1***: Tần suất kiểm tra các bản cập nhật ***(khuyến nghị để automatic updates)***

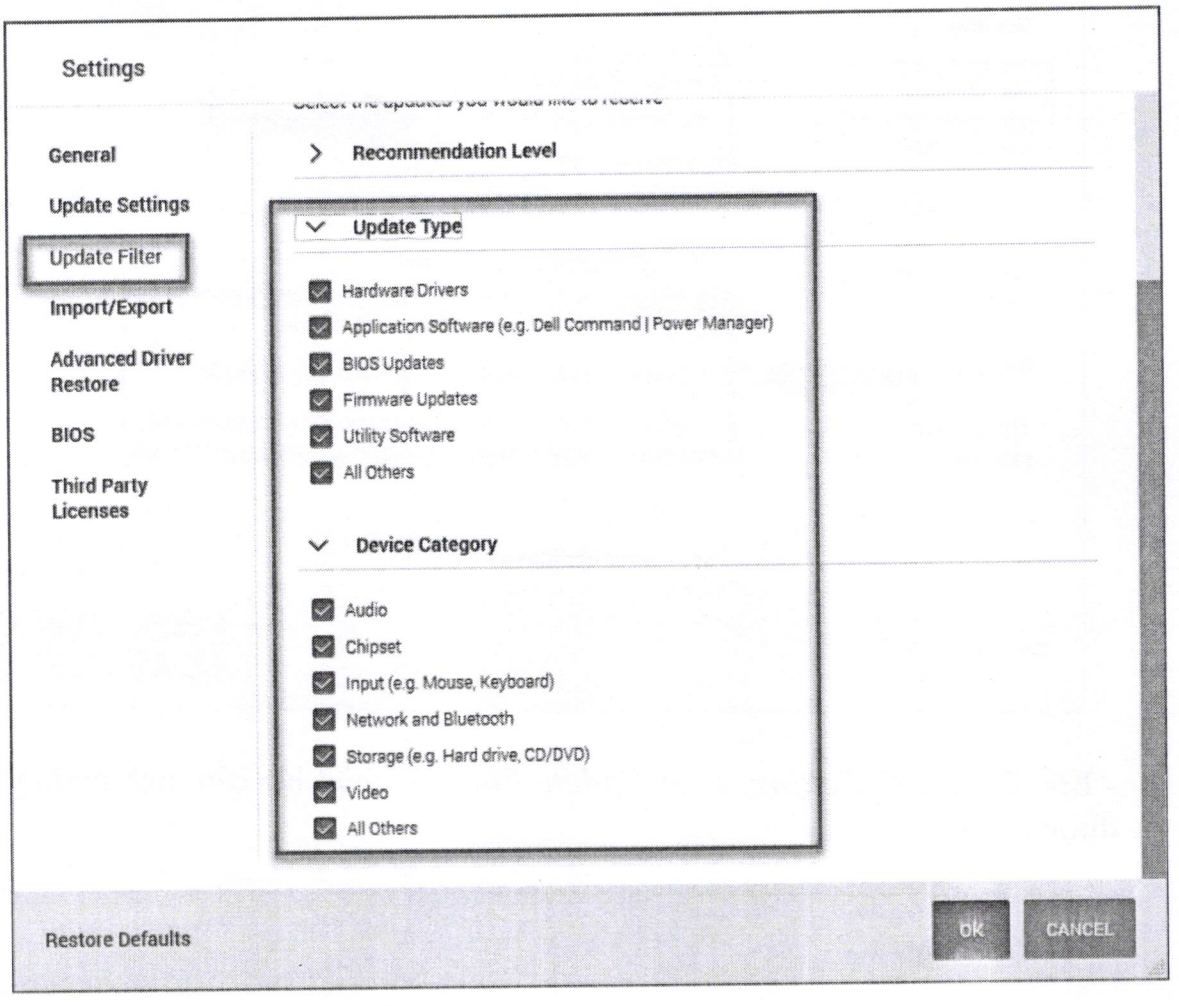
+ ***Mục 2:*** Cho phép ứng dụng thực hiện hành động khi phát hiện ra bản cập nhật mới ***(khyến nghị chọn Download Updates)***



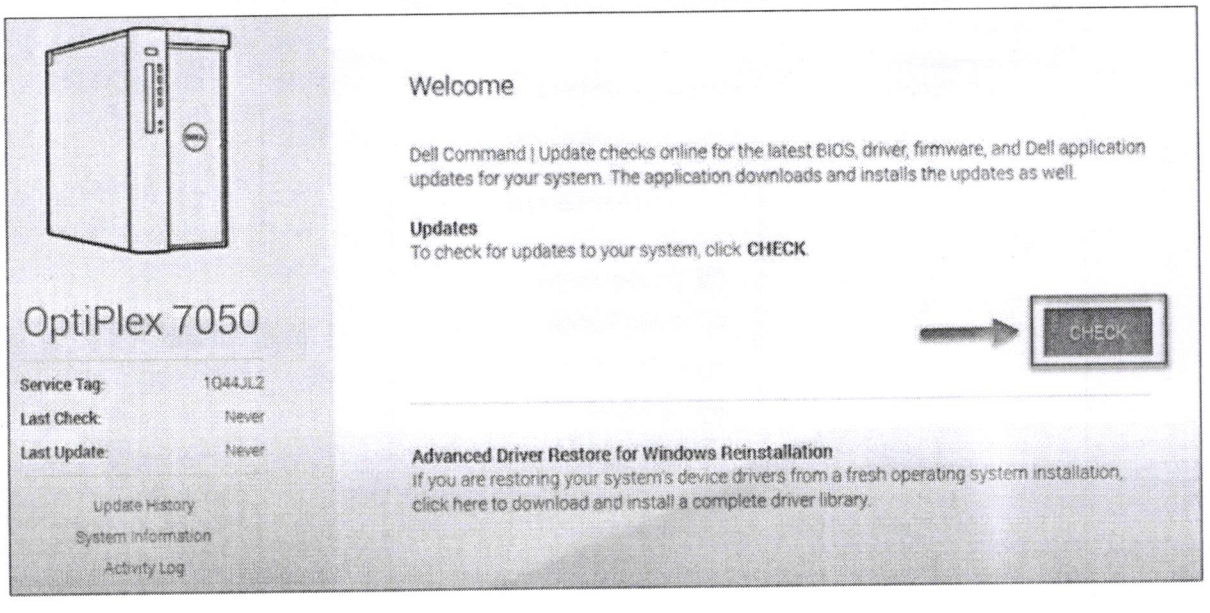
- **B5:** Tại cửa sổ ***Setting***, chọn ***Update Filter*** để thiết lập cấu hình những bản vá được tải về



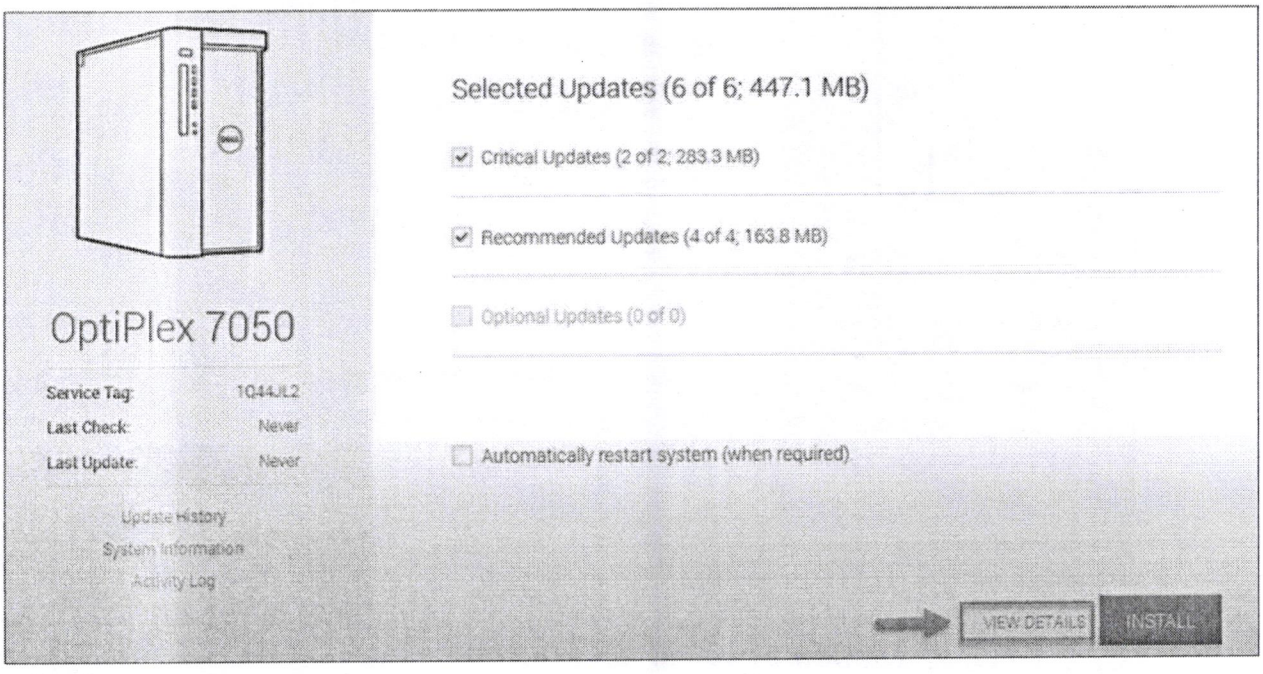
+ ***Recommendation level:*** Có thể tùy chọn chỉ cập nhật những bản vá quan trọng
+ ***Update Type/ Device Category***: Chọn những phần cần tải bản cập nhật (BIOS, driver phần cứng,…)



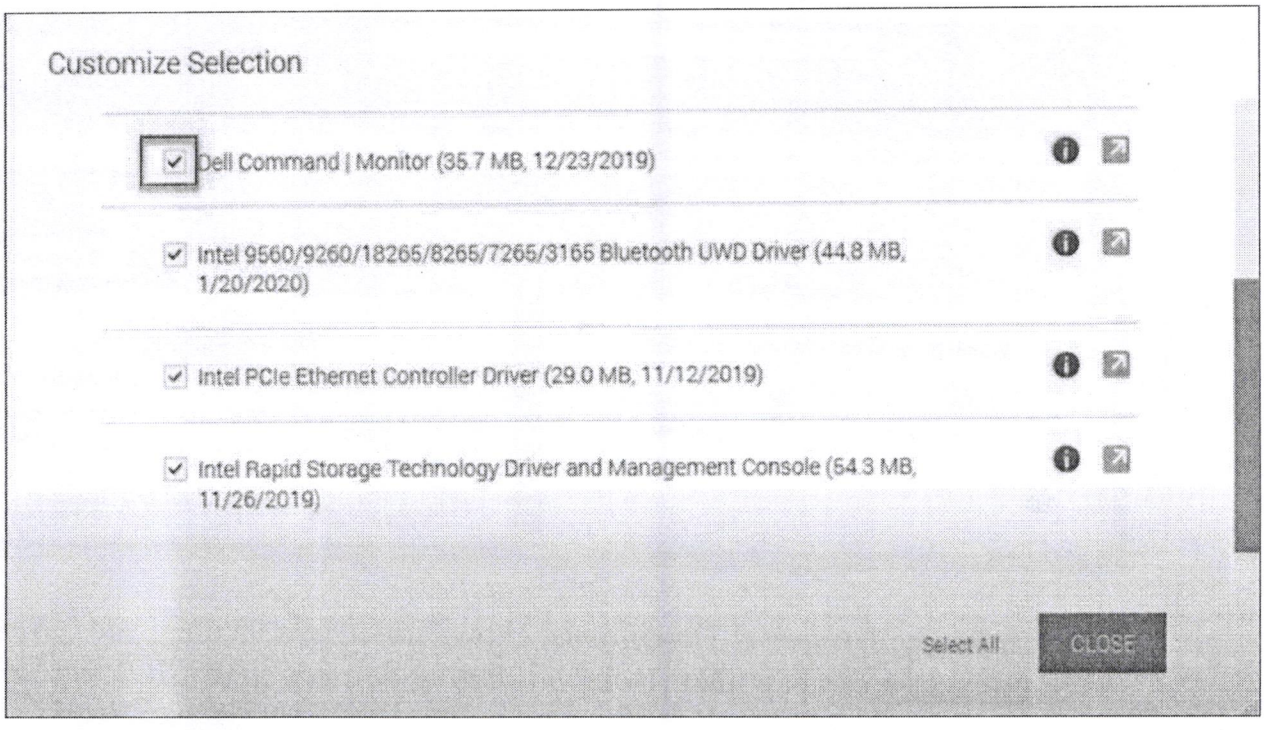
- **B6:** Sau khi thiết lập xong, chọn ***OK,*** sau đó chọn ***Check*** để kiểm tra các bản cập nhật



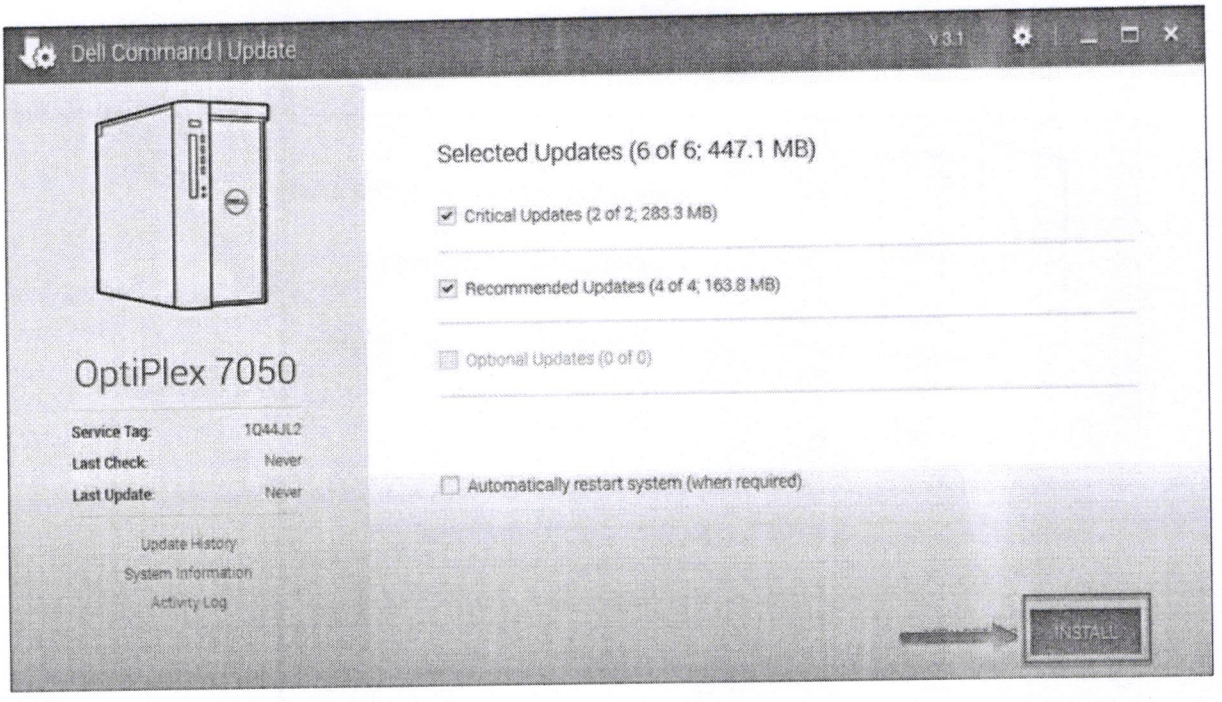
- ***B7:*** Sau khi kiểm tra, chọn ***View Details*** để kiểm tra thông tin các bản cập nhật



+ Chọn các bản cập nhật được cài/không được cài vào máy bằng cách tích vào ô đầu mỗi bản cập nhật

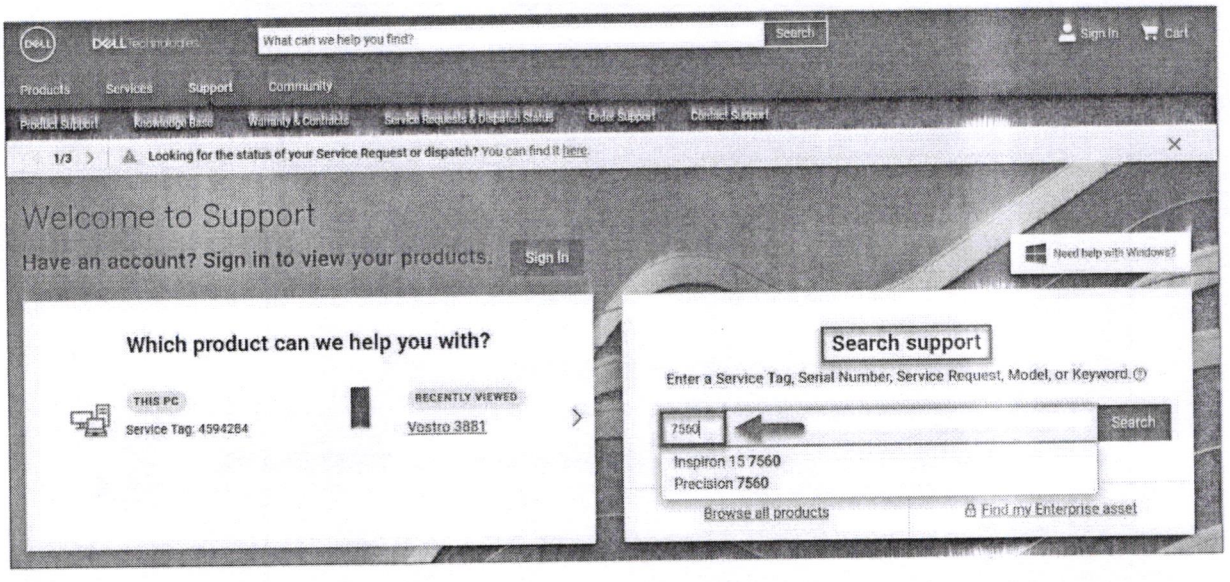


- ***B8:*** Chọn ***INSTALL*** để cài đặt các bản vá được lựa chọn, khởi động lại máy tính nếu ứng dụng yêu cầu



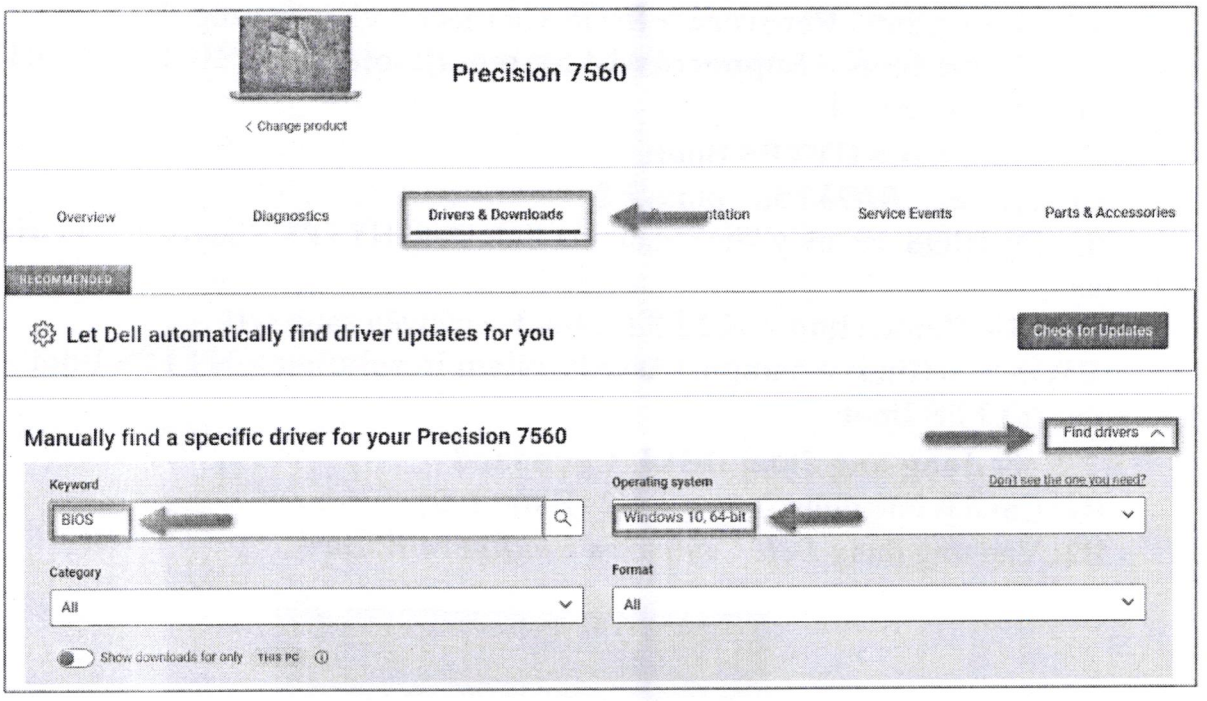
3.1.2. Cách 2: Tải bản vá và cài đặt thủ công

- **B1**: Truy cập trang: https://www.dell.com/support/home/en-vn và tìm kiếm theo ***Serivce Tag*** hoặc ***Model*** của máy tính cần tải bản cập nhật tại mục ***Search Support***

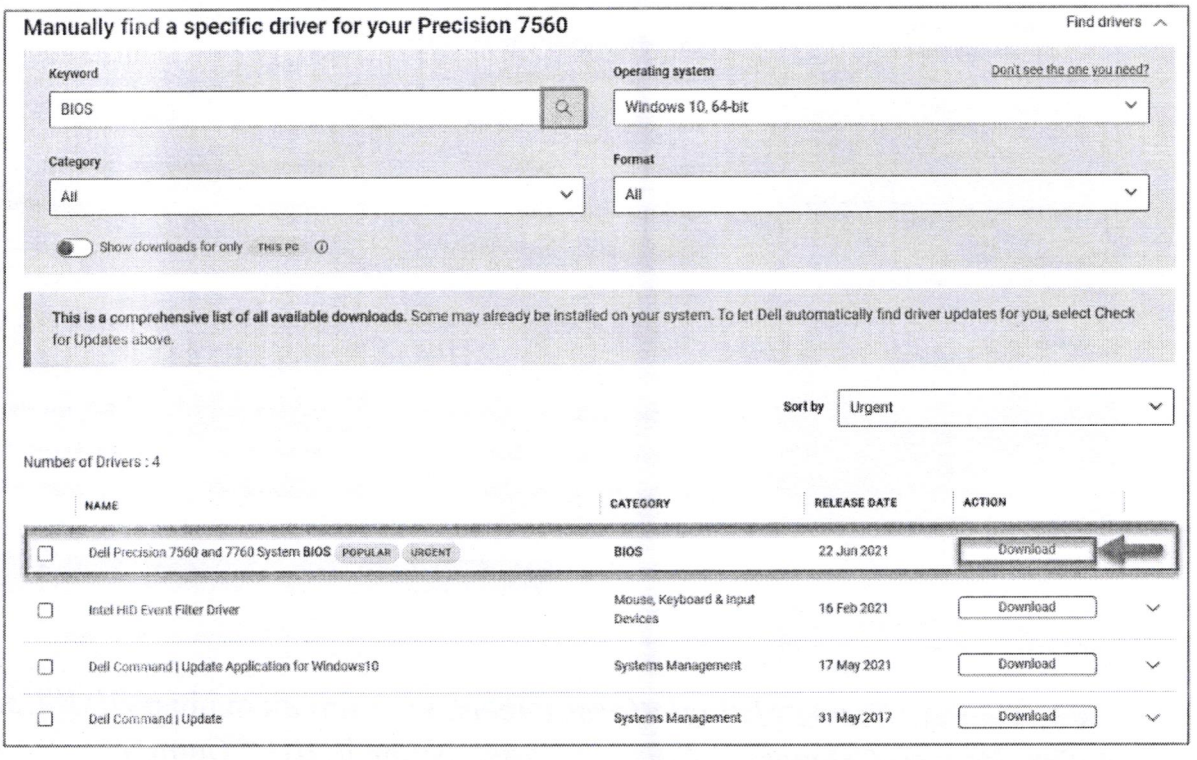


- **B2:** Chọn mục ***Drivers & Downloads,*** chọn ***Find drives*** và nhập vào ô ***Keyword*** thông tin bản vá cần cập nhật *(trong bài hướng dẫn cập nhật BIOS nên sẽ nhập BIOS vào ô Keyword)*

+ Chọn hệ điều hành đang sử dụng của máy



- **B3:** Chọn bản vá được khuyến nghị *(Kiểm tra ngày Release)* và chọn ***Download***



- **B4**: Cài đặt bản vá vừa tải về và khởi động lại máy nếu được yêu cầu

3.2. Đối với lựa chọn không cập nhật bản vá BIOS

3.2.1. Truy cập vào BIOS thay đổi cấu hình

a) Tắt tính năng BIOS Connect:

- **B1**: Truy cập ***BIOS*** bằng phím ***F2***
- **B2:** Do BIOS các máy khác nhau mà tính năng BIOS Connect nằm ở vị trí khác nhau:

+ **BIOS > Update, Recovery > BIOS Connect >** chuyển sang **Off**
+ **BIOS > Settings > SupportAssist System Resolution > BIOS Connect >** Bỏ chọn **BIOSConnect**

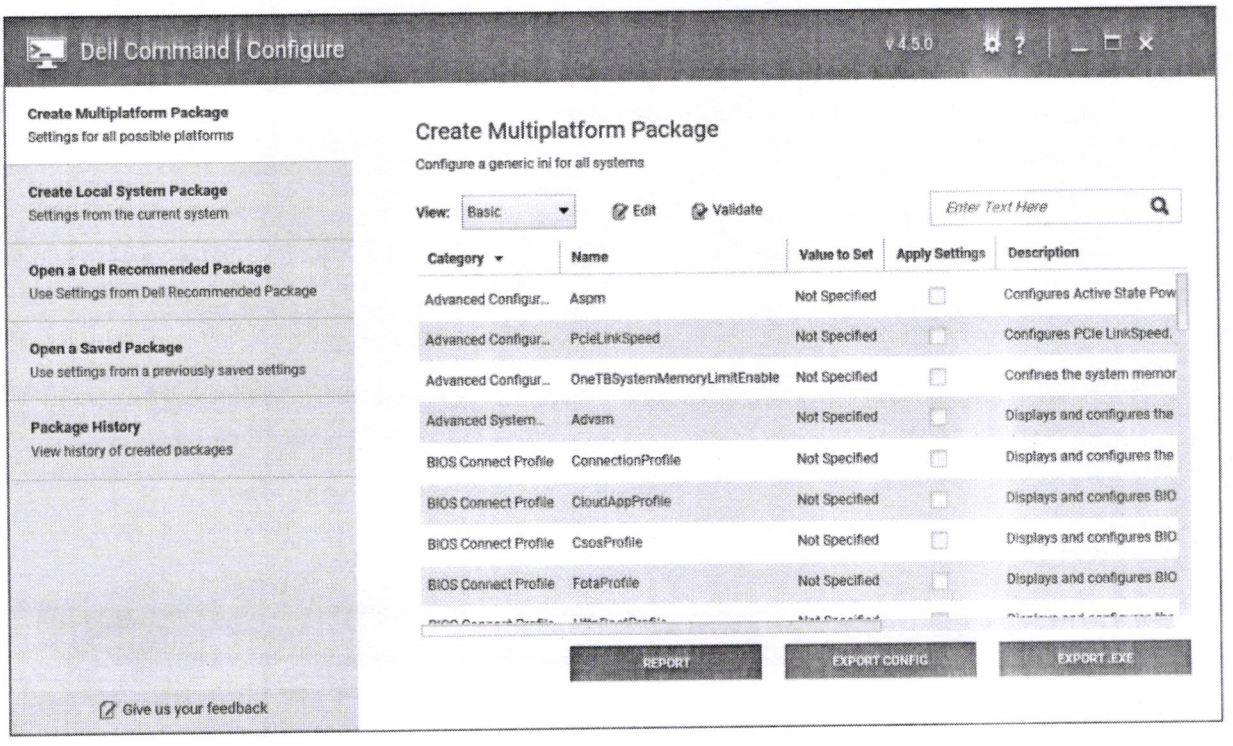
b) Tắt tính năng HTTPS Boot:

- **B1**: Truy cập ***BIOS*** bằng phím ***F2***
- **B2:** Do BIOS các máy khác nhau mà tính năng HTTPS Boot nằm ở vị trí khác nhau:

+ **BIOS > Connection > HTTP (s) Boot >** chuyển sang **Off**
+ **BIOS > Settings > SupportAssist System Resolution > HTTPS Boot >** Bỏ chọn **HTTPS Boot**

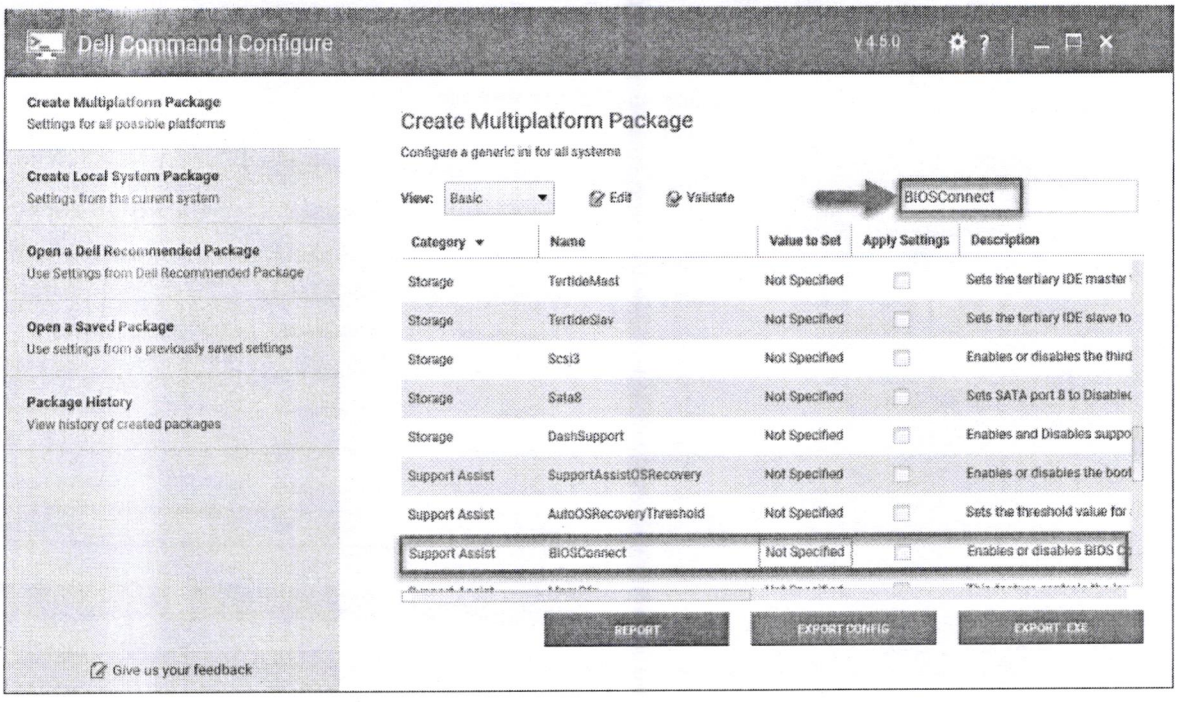
3.2.2. Sử dụng ứng dụng DELL Command

- **B1**: Cài đặt ứng dụng ở mục 1.1.2 (Bước 1, 2)
- **B2**: Vào ứng dụng ***Dell Command Configure Wizard***

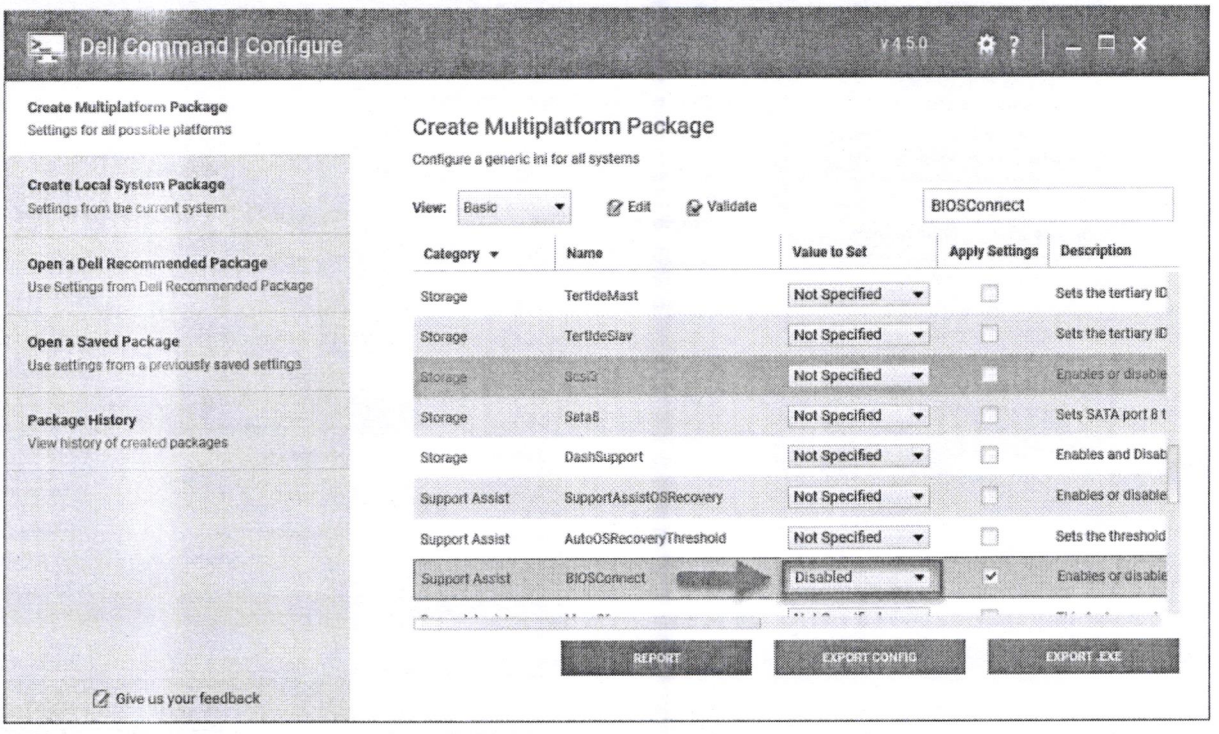


- **B3**: Tại mục ***Create Multiplatform Packet***, tại ô tìm kiếm nhập ***BIOSConnect***

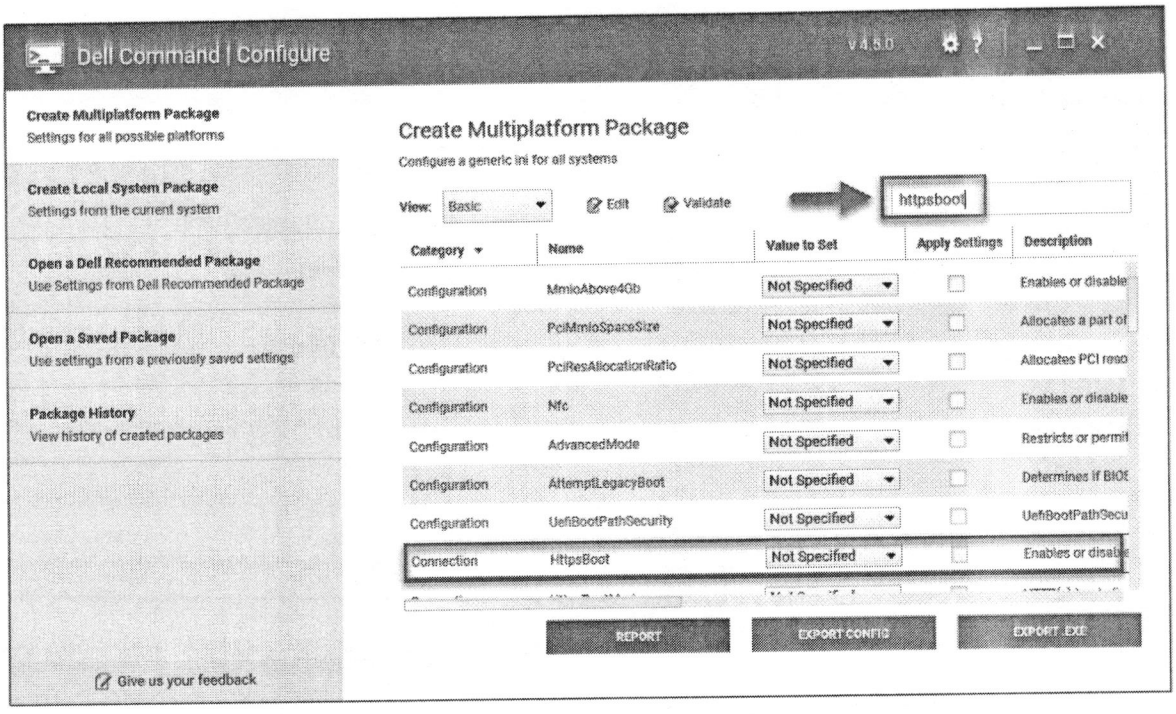
+ Tìm dòng có ***Category*** là ***Support Assist***; ***Name*** là ***BIOSConnect***



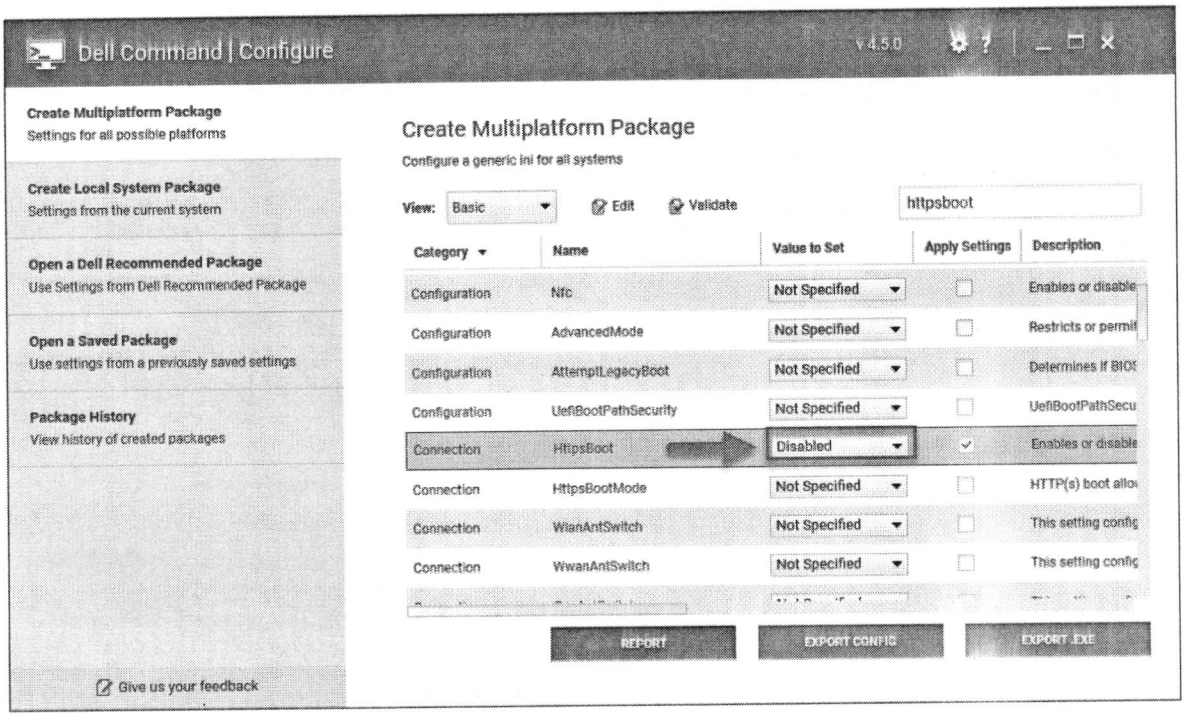
+ Tại cột ***Value to Set*** chọn ***Disable***



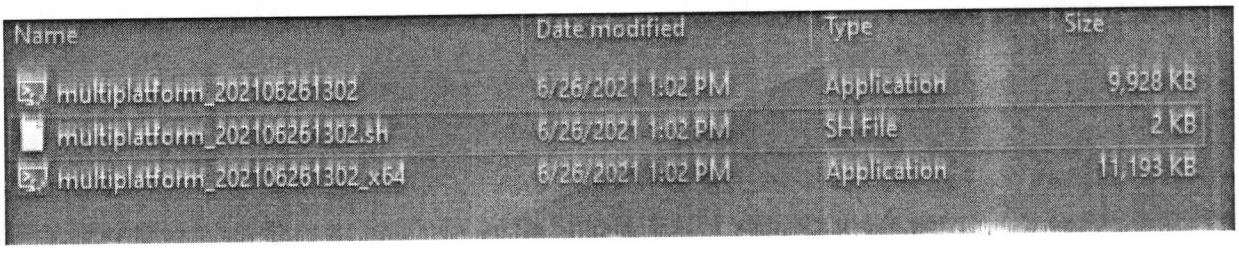
- **B4:** Tại mục ***Create Multiplatform Packet***, tại ô tìm kiếm nhập ***HTTPSBoot***
+ Tìm dòng có ***Category*** là ***Connection***; ***Name*** là ***HTTPSBoot***



+ Tại cột ***Value to Set*** chọn ***Disable***



- **B5**: Sau khi thiết lập ***BIOSConnect*** và ***HTTPSBoot***, chọn ***EXPORT.EXE*** và chọn nơi lưu file cấu hình



- **B6**: Chạy file cấu hình vừa xuất ra và khởi động lại máy để hoàn tất thiết lập cấu hình cho BIOS

4. Tài liệu tham khảo

https://www.dell.com/support/kbdoc/en-vn/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-bioscconnect-feature-and-https-boot-feature