

UBND THÀNH PHỐ HẢI PHÒNG  
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2165/STTTT-CNTT

Hải Phòng, ngày 23 tháng 10 năm 2020

V/v nguy cơ tấn công vào các cơ quan  
tổ chức qua lỗ hổng trong VMware vCenter.


Kính gửi:

- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện;
- Các tổ chức, doanh nghiệp trên địa bàn.

Ngày 16/10/2020, Cục An toàn thông tin có Công văn số 924/CATTT-NCSC về việc nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng trong VMware vCenter, hướng dẫn cách khắc phục lỗ hổng trên (gửi kèm văn bản).

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị kiểm tra, rà soát hệ thống công nghệ thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trong VMware vCenter và thực hiện các biện pháp xử lý, khắc phục tại đơn vị và các cơ quan trực thuộc theo hướng dẫn của Cục An toàn thông tin tại Công văn số 924/CATTT-NCSC.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./. 

**Nơi nhận:**

- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GD, các PGĐ Sở;
- TT.TTTT;
- Công TTĐT Sở, Cổng Tin tức TP;
- Lưu: VT, CNTT.

**KT. GIÁM ĐỐC**  
**PHÓ GIÁM ĐỐC**  


**Lê Văn Kiên**



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: 924 /CATTT-NCSC  
V/v nguy cơ tấn công vào các cơ quan tổ  
chức qua lỗ hổng trong VMware vCenter

Hà Nội, ngày 16 tháng 10 năm 2020

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.

Qua công tác giám sát an toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin phát hiện xu hướng khai thác lỗ hổng trong VMware vCenter, cho phép đối tượng tấn công đọc tệp tùy ý. Theo đánh giá sơ bộ VMware vCenter là ứng dụng được sử dụng tại rất nhiều cơ quan tổ chức trong việc quản lý tập trung các máy ảo và máy chủ ESX/ESXi (có ít nhất hơn 20 hệ thống máy chủ đang hoạt động công khai trên Internet, chưa kể nhiều hệ thống không công khai).

Đầu tháng 10, Trung tâm Giám sát an toàn không gian mạng quốc gia phát hiện một số mã khai thác đã được công khai trên Internet, những mã khai thác này có thể sử dụng để tấn công vào các máy chủ VMware vCenter qua đó kiểm soát hệ thống thông tin của các cơ quan tổ chức trong các chiến dịch tấn công nguy hiểm.

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 yêu cầu đơn vị triển khai quyết liệt một số khuyến nghị sau:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên và có phương án xử lý, khắc phục lỗ hổng. Quý đơn vị nên cập



nhật, nâng cấp lên phiên bản VMware vCenter mới nhất để khắc phục lỗ hổng bảo mật nói trên và các lỗ hổng bảo mật mới phát hiện khác. Lỗ hổng bảo mật này đã được vá tại VMware vCenter phiên bản 6.5u1.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng. Đối với các có quan tổ chức có nhân sự kỹ thuật tốt có thể thử nghiệm xâm nhập vào hệ thống thông qua lỗ hổng này.

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, điện thoại 02432091616, thư điện tử: [ais@mic.gov.vn](mailto:ais@mic.gov.vn).

Trân trọng./.

**Nơi nhận:**

- Như trên;
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

**SAO Y BẢN CHÍNH**  
Ngày 23 tháng 10 năm 2020

**KT. CỤC TRƯỞNG  
PHÓ CỤC TRƯỞNG**

Ký bởi: Cục An toàn thông tin  
Cơ quan: Bộ Thông tin và Truyền thông  
Thời gian ký: 16/10/2020 16:32:42



**Nguyễn Khắc Lịch**

**CHÁNH VĂN PHÒNG**  
*Nguyễn Thị Thu Hà*



**Phụ lục**  
**Hướng dẫn chi tiết vá lỗ hổng bảo mật**

(Kèm theo Công văn số /CATTT-NCSC ngày / /2020)

Lỗ hổng tồn tại trong phiên bản VMware 6.5.0a-f. Tuy nhiên qua công tác rà soát của Trung tâm Giám sát an toàn không gian mạng quốc gia, lỗ hổng này ảnh hưởng đến cả phiên bản từ 6.0.0 đến 6.5.0 và có thể ảnh hưởng cả đến các phiên bản cũ hơn. Vì vậy để tránh nguy cơ bị khai thác, Trung tâm NCSC khuyến nghị các quản trị viên cập nhật hệ thống lên phiên bản VMware vCenter mới nhất. Thực hiện vá lỗ hổng bảo mật này theo các cách sau:

**Cách 1:** Nâng cấp lên phiên bản VMware vCenter mới nhất. Thực hiện theo hướng dẫn của nhà phát triển tại: <https://my.vmware.com/group/vmware/patch>.

**Cách 2:** Cập nhật các bản vá bảo mật đã biết. Mỗi bản vá sẽ có cách cập nhật và sự tương thích khác nhau, cần thực hiện theo hướng dẫn của nhà phát triển.

- VMware phân phối các bản vá có sẵn ở 2 dạng: mô hình dựa trên ISO và mô hình vá dựa trên URL.

Bản vá dạng hình ảnh ISO có thể tải tại:

<https://my.vmware.com/group/vmware/patch>

Quản trị viên cũng có thể tải các bản vá dạng ZIP tại:

<https://my.vmware.com/web/vmware/downloads> và xây dựng 1 kho lưu trữ tùy chỉnh trên máy chủ web cục bộ, tên tệp tải xuống là `VMware-vCenter-Server-Appliance- product_version - build_number -updaterepo.zip`

Dưới đây là chi tiết các bước cập nhật cho phiên bản VMware vCenter 6.5u1:

B1: Truy cập vào trang web nhà phát triển và tải tệp:

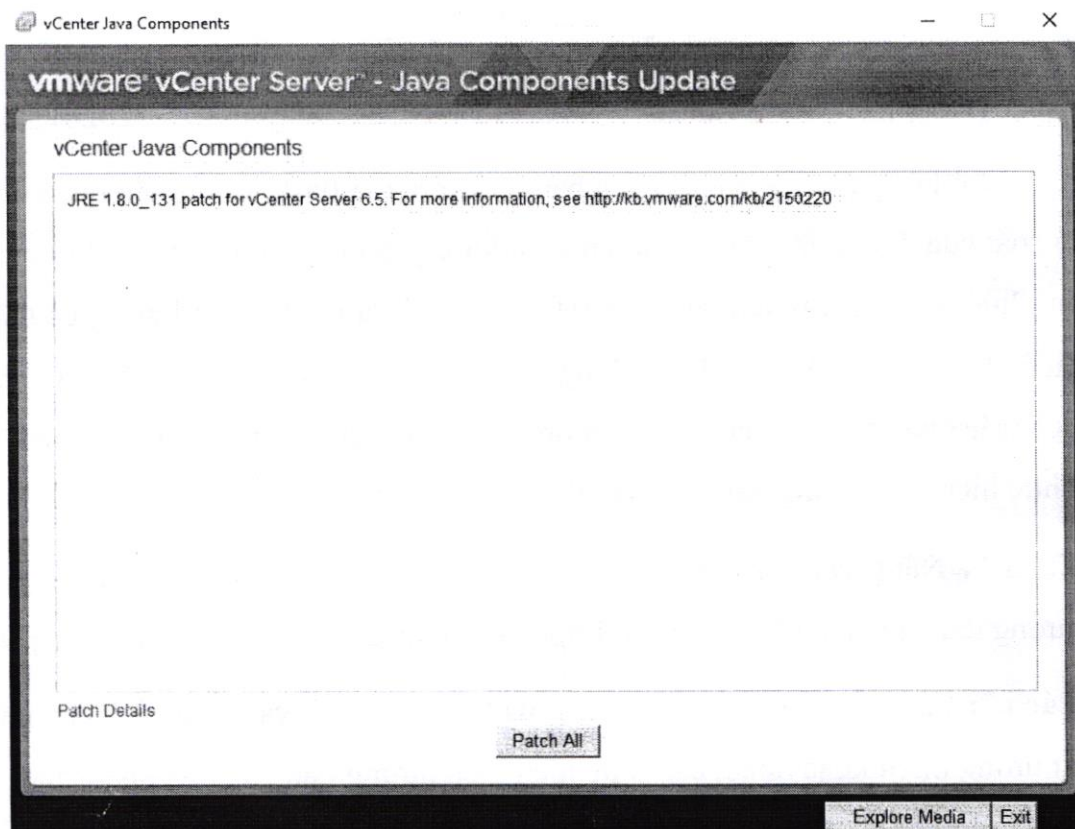
VMware-vCenter-Server-Appliance-6.5.0.12000-7116595-patch-FP.iso

B2: Đưa bản vá đã tải xuống vào hệ thống cài đặt cấu hình vCenter Server

B3: Bấm đúp vào ISO\_mount\_directory / autorun.exe

B4: Nhấp vào **Patch All**





Thông tin tham khảo thêm tại:

<https://kb.vmware.com/s/article/2150220>

**Cách 3:** Trong trường hợp chưa thể nâng cấp kịp thời cần thực hiện biện pháp để ngăn chặn tấn công khai thác lỗ hổng trên bằng cách sử dụng hệ thống tường lửa.