Phụ lục

HƯỚNG DẪN CHI TIẾT VÁ LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /STTTT-TTCNTT&TT ngày /10/2020 của Sở Thông tin và Truyền thông)

1. Phiên bản tồn tại lỗ hổng bảo mật

STT	Phiên bản VMware	CVE
1	VMware vCenter Server 6.7	2020-3952
2	VMware vCenter Server 6.5	2019-5534
3	VMware vCenter Server 6.0	

2. Hướng dẫn khắc phục lỗ hổng bảo mật

Thực hiện cập nhật hệ thống phiên bản VMware vCenter lên phiên bản mới nhất, 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:

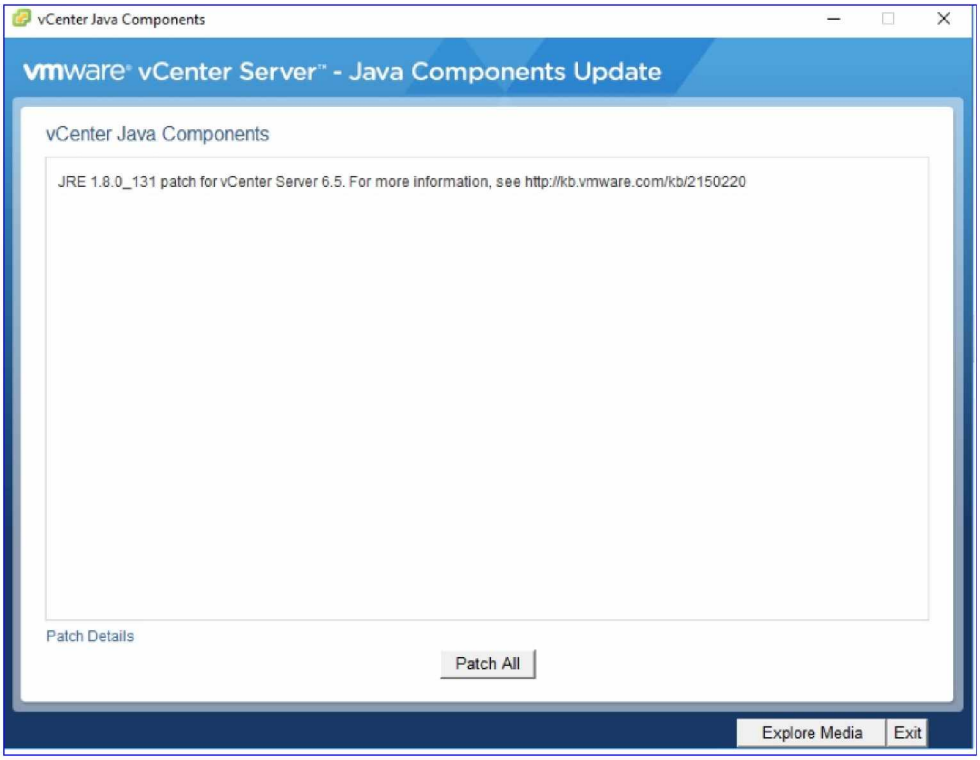
Bước 1: Truy cập vào trang web nhà phát triển và tải tệp

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

Bước 2: Đưa bản vá đã tải xuống vào hệ thống cài đặt cấu hình vCenter Server

Bước 3: Bấm đúp vào ISO_mount_directory / autorun.exe

Bước 4: 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.

---Hết---