BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 44 /TTCNTT-KTHT
V/v cảnh báo lỗ hổng nghiêm trọng trong sản phẩm VMware

Hà Nội, ngày 08 tháng 3 năm 2021

Kính gửi: Các đơn vị có hệ thống công nghệ thông tin trực thuộc Bộ

Theo nội dung Công văn số 45/BCY-CNTTGSM ngày 26/2/2021 về việc cảnh báo lỗ hổng nghiêm trọng trong sản phẩm VMware, Ban Cơ yếu Chính phủ đã ghi nhận lỗ hổng nghiêm trọng cho phép thực thi mã từ xa với đặc quyền không hạn chế trên các máy chủ vCenter (CVE-2021-21972) đối với các phiên bản VMware vCenter Server từ 6.5 đến 7.0 và VMware Cloud Foundation (vCenter Server) từ 3.X đến 4.X. Kẻ tấn công có thể lợi dụng lỗ hổng để chiếm quyền điều khiển toàn bộ hệ thống ảo hóa sử dụng vCenter.

Ngoài ra trên phiên bản VMware ESXi từ 6.5 đến 7.0 cũng tồn tại lỗ hổng cho phép kẻ tấn công thực thi các mã lệnh từ xa (CVE-2021-21974).

Theo nhận định, các lỗ hổng trên ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan Đảng, Nhà nước và các tổ chức kinh tế - xã hội, do các sản phẩm của VMware hiện đang được sử dụng rất phổ biến để ảo hóa hệ thống.

Nhằm đảm bảo an toàn thông tin cho các hệ thống sử dụng những sản phẩm VMware như trên, Trung tâm Công nghệ thông tin đề nghị các Quý đơn vị:

1. Khẩn trương rà soát, kiểm tra lại phiên bản VMware Cloud Foundation, VMware ESXi và VMware vCenter để phát hiện các máy chủ bị ảnh hưởng và xử lý kịp thời các máy chủ có khả năng bị đối tượng tấn công khai thác thông qua lỗ hổng trên.

2. Cập nhật bản vá hoặc khắc phục lỗ hổng theo hướng dẫn *(chi tiết trong Phụ lục đính kèm).*

3. Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chuyên trách về an toàn thông tin để kịp thời phát hiện và xử lý các nguy cơ tấn công mạng.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để biết);
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng và hướng dẫn khắc phục
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

STT	Tên lỗ hổng	Sản phẩm ảnh hưởng	Phiên bản	Phiên bản đã vá lỗ hổng	Hướng dẫn vá lỗ hổng
1	VSphere Client (HTML5) chứa lỗ hổng thực thi mã từ xa trong plugin vCenter Server (CVE -2021-21972)	vCenter Server	6.5	6.5 U3n	https://kb.vmware.com/s/article/82374
		vCenter Server	6.7	6.7 U3l	https://kb.vmware.com/s/article/82374
		vCenter Server	7.0	7.0 U1c	https://kb.vmware.com/s/article/82374
		Cloud Foundation (vCenter Server)	3.x	3.10.1.2	https://kb.vmware.com/s/article/82374
		Cloud Foundation (vCenter Server)	4.x	4.2	https://kb.vmware.com/s/article/82374
2	ESXi OpenSLP chứa lỗ hổng tràn heap (heap-overflow) (CVE -2021-21974)	ESXi	6.5	ESXi650-202102101-SG	https://kb.vmware.com/s/article/76372
		ESXi	6.7	ESXi670-202102401-SG	https://kb.vmware.com/s/article/76372
		ESXi	7.0	ESXi70U1c-17325551	https://kb.vmware.com/s/article/76372
		Cloud Foundation (ESXi)	3.x		https://kb.vmware.com/s/article/76372
		Cloud Foundation (ESXi)	4.x	4.2	https://kb.vmware.com/s/article/76372

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số số /TTCNTT-KTHT ngày / /2021)

STT	Tên đơn vị
1	Cục Thông tin khoa học và công nghệ quốc gia
2	Cục Sở hữu trí tuệ
3	Tổng cục Tiêu chuẩn Đo lường Chất lượng
4	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
5	Viện Năng lượng nguyên tử Việt Nam
6	Viện Khoa học sở hữu trí tuệ
7	Quỹ phát triển khoa học và công nghệ quốc gia
8	Cục An toàn bức xạ và hạt nhân
9	Quỹ đổi mới công nghệ quốc gia
10	Ban Quản lý Khu công nghệ cao Hòa Lạc