UBND TỈNH NINH BÌNH
SỞ NÔNG NGHIỆP VÀ PTNT

Số: 2535 /SNN-VP
V/v triển khai rà quét, khắc phục nguy cơ tấn công mạng vào các cơ quan, tổ chức qua lỗ hổng trong VMware vCenter

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

Ninh Bình, ngày 06 tháng 11 năm 2020

Kính gửi: Các đơn vị trực thuộc Sở

Sở Nông nghiệp và Phát triển nông thôn nhận được Văn bản số 1468/STTTT-CNTT ngày 23/10/2020 của Sở Thông tin và Truyền thông về việc triển khai rà quét, khắc phục nguy cơ tấn công mạng vào các cơ quan, tổ chức qua lỗ hổng trong VMware vCenter.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị trực thuộc Sở, Sở Nông nghiệp và Phát triển nông thôn yêu cầu các đơn vị triển khai thực hiện một số nội dung sau:

1. 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. Cập nhật, nâng cấp lên phiên bản VMware vCenter 6.5ul mới nhất *(Hướng dẫn cập nhật chi tiết tại Phụ lục 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.

Trong quá trình thực hiện nếu cần hỗ trợ đề nghị liên hệ: Ông Quách Hoàng Thạch, Quản trị mạng - Văn phòng Sở, điện thoại: 0915.386.012.

Sở Nông nghiệp và Phát triển nông thôn yêu cầu các đơn vị nghiêm túc thực hiện các nội dung trên./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở (để b/c);
- Trang Thông tin điện tử của Sở;
- Lưu: VT, VP.

MC

TL.GIÁM ĐỐC
CHÁNH VĂN PHÒNG

Ký bởi: Sở Nông nghiệp và Phát triển Nông thôn
Cơ quan: Tỉnh Ninh Bình
Thời gian ký: 06/11/2020 16:04:28

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH NINH BÌNH

Bùi Xuân Thư

Phụ lục

HƯỚNG DẪN CHI TIẾT VÁ LỖ HỔNG BẢO MẬT

(Kèm theo Văn bản số /SNN-VP ngày / /2020 của Sở Nông nghiệp và PTNT)

Lỗ hổng tồn tại trong phiên bản Vmware 6.5.0a-f. Tuy nhiên qua công tácràsoát của Trung tâm Giám sát an toàn không gian mạng quốc gia, lỗ hổng nàyảnh hưởng đến cả phiên bản từ 6.0.0 đến 6.5.0 và có thể ảnh hưởng cả đến cácphiên bản cũ hơn. Vì vậyđể tránh nguy cơ bị khai thác, Sở Thông tin và Truyền thông khuyếnnghị các quản trị viên cậpnhật 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 theohướng 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 vàsự 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 môhình vá dựa trên URL.

+ Bản vá dạng hình ảnh ISO có thể tải tại địa chỉ:

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

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

https://my.vmware.com/web/vmware/downloads và xây dựng 1 kho lưu trữ tùychỉnh trên máy chủ web cục bộ, tên tệp tải xuống là `VMware-vCenter-ServerAppliance-`*`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 đểngăn chặn tấn công khai thác lỗ hổng trên bằng cách sử dụng hệ thống tường lửa.