UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 470 /STTTT-CNTT
Về việc cảnh báo lỗ hổng bảo mật trên sản phẩm vCenter Server

Tuyên Quang, ngày 14 tháng 6 năm 2021

Kính gửi:
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông.

Căn cứ Văn bản số 143/BCY-CNTTGSM ngày 03/6/2021 của Ban Cơ yếu Chính phủ về việc cảnh báo lỗ hổng bảo mật nghiêm trọng trên sản phẩm vCenter Server;

Thực hiện Văn bản số 1822/UBND-THCB ngày 09/6/2021 của Ủy ban nhân dân tỉnh Tuyên Quang về việc thực hiện Văn bản số 143/BCY-CNTTGSM ngày 03/6/2021 của Ban Cơ yếu Chính phủ; Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh việc khai thác lỗ hổng bảo mật trên sản phẩm vCenter Server, cụ thể như sau:

I. Thông tin về lỗ hổng bảo mật trên sản phẩm vCenter Server

Theo khuyến cáo bảo mật VMS A 2021-0010 của Công ty Vmware vào ngày 25/5/2021, trong đó có thông báo chi tiết đến lỗ hổng CVE-2021-21985 trong vSphere Client (HTML 5) một thành phần của vCenter Server và Vmware Cloud Foundation. Lỗ hổng phát sinh do lỗi xác thực thiếu kiểm tra tham số đầu vào trong tính năng của Virtual SAN Health Check (tính năng này được bật mặc định trong vCenter Server). Lỗ hổng này thực thi qua cổng 443 (https), cho phép kẻ tấn công thực hiện các lệnh với đặc quyền cao nhất trong hệ thống và không bị hạn chế bất tỳ truy cập nào đối với máy chủ cài hệ điều hành vCenter Server. Theo đánh giá của CVSSv3 mức độ nguy hiểm của" CVE-202 V-21985 là 9.8 (đặc biệt nghiêm trọng). Đây là nguy cơ có thể gây thiệt hại lớn đến các hệ thống của mạng của các cơ quan, đơn vị đang sử dụng hệ điều hành vCenter Server.

II. Các giải pháp phòng, tránh

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, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện các giải pháp sau:

1. Rà soát xác minh hệ thống có sử dụng vCenter Server để phát hiện và xử lý kịp thời các lỗ hổng bảo mật.

2. Cập nhật bản vá hoặc khắc phục lỗ hổng bảo mật đồng thời thường xuyên thực hiện kiểm tra đánh giá, bảo đảm an toàn thông tin.

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

(Có Phụ lục thông tin về lỗ hổng bảo mật trên sản phẩm vCenter Server gửi kèm)

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Sở Thông tin và Truyền thông
14-06-2021 16:47:56 +07:00

Nguyễn Văn Hiến

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG BẢO MẬT TRÊN SẢN PHẨM VCENTER SERVER

(Kèm theo Công văn số 470/STTTT-CNTT ngày 14 /6/2021 của Sở Thông tin và Truyền thông)

STT	Mô tả	Nội dung
1	Các phiên bản bị ảnh hưởng	- vCenter Server 6.5 - vCenter Server 6.7 - vCenter Server 7.0 - Cloud Foundation (vCenter Server) 3.x - Cloud Foundation (vCenter Server) 4.x
2	Bản vá	Thông tin về bản vá lỗ hổng theo đường link: https://www.vmware.com/security/advisories/VMSA-2021-0010.html Trong trường hợp đặc biệt nếu không thể vá ngay lập tức, quý cơ quan có thể tắt tính năng Virtual San Health Check tại đường dẫn: https://kb.vmware.com/s/articie/83829
3	Cách thức kiểm tra đầu vào	Để kiểm tra hệ thống bị tấn công bởi lỗ hổng CVE-2021-21985, có thể kiểm log trong các thư mục theo đường dẫn mặc định: - vCenter Server 6.X và phiên bản cao hơn trên Windows server: C: \ProgramData\VMware\vCenterServer\Logs\ - vCenter Server Appliance 6.x: /var/log/vmware/ - vCenter Server Appliance 6.x flash: /var/log/vmware/vsphere-client - vCenter Server Appliance 6.x HTML5: /var/log/vmware/vsphere-ui hoặc cấu hình của người dùng có dấu hiệu như sau:

		
4	Thông tin chi tiết	Thông tin chi tiết về lỗ hổng này có tại các đường link dưới đây: - https://www.vmware.com/security/advisories/VMSA-2021-0010. html - https://blogs.vmware.com/vsphere/202l/05/vmsa-2021-0010.html - https://core.vmware.com/resource/vmsa-2021-0010-faq.