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: *73* /TTCNTT-KTHT
V/v cảnh báo lỗ hổng bảo mật trong sản phẩm VMware

Hà Nội, ngày 2 tháng 04 năm 2021

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

Ngày 30/03/2021, VMware tiếp tục công bố 02 lỗ hổng bảo mật **(CVE-2021-21975, CVE-2021-21983)** trong phần mềm VMware vRealize Operations Manager, cho phép đối tượng tấn công thực hiện tấn công giả mạo yêu cầu từ phía máy chủ (SSRF) để đánh cắp thông tin xác thực của quản trị viên, cài cắm tệp tin độc hại, từ đó chiếm quyền kiểm soát toàn bộ hệ thống. Các lỗ hổng này ảnh hưởng đến các sản phẩm vRealize Operations Manager, VMware Cloud Foundation (vROps), vRealize Suite Lifecycle Manager (vROps) (thông tin chi tiết về các lỗ hổng có tại phụ lục kèm theo).

Theo đánh giá sơ bộ, phần mềm VMware vRealize Operations Manager thường được sử dụng nhiều trong hệ thống của các cơ quan tổ chức doanh nghiệp để hỗ trợ việc giám sát các thiết bị VMware, cải thiện hiệu suất ứng dụng, nâng cao hiệu quả và giảm thiểu gián đoạn.

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Tham khảo hướng dẫn tại phụ lục kèm theo.

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 cơ quan tổ chức có nhân sự kỹ thuật tốt có thể thử nghiệm xâm nhập vào hệ thống thông qua lỗ hổng này.

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 b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

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

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong VMware
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

1. Thông tin các lỗ hổng bảo mật

1.1. Lỗ hổng bảo mật CVE-2021-21975

- Điểm CVSS: 8.6 (cao)

- Chức năng vRealize Operations Manager API tồn tại lỗ hổng SSRF cho phép đối tượng tấn công không cần xác thực có thể đánh cắp thông tin xác thực của quản trị viên.

1.2. Lỗ hổng bảo mật CVE-2021-21983

- Điểm CVSS: 7.2 (cao)

- Chức năng vRealize Operations Manager API tồn tại lỗ hổng Arbitrary File Write cho phép đối tượng tấn công với quyền quản trị cao có thể thực hiện ghi tệp tùy ý lên hệ thống (hệ điều hành photon).

2. Hướng dẫn khắc phục:

Cách 1: Thực hiện cập nhật bản vá theo hướng dẫn của nhà cung cấp. Tham khảo bảng sau:

Sản phẩm	Phiên bản bị ảnh hưởng	Tham khảo link bản vá
vRealize Operations Manager	8.3.0	https://kb.vmware.com/s/article/83210
	8.2.0	https://kb.vmware.com/s/article/83095
	8.1.1, 8.1.0	https://kb.vmware.com/s/article/83094
	8.0.1, 8.0.0	https://kb.vmware.com/s/article/83093
	7.5.0	https://kb.vmware.com/s/article/82367
Vmware Cloud Foundation (vROps)	4.x	https://kb.vmware.com/s/article/83260
	3.x	https://kb.vmware.com/s/article/83260
	8.x	https://kb.vmware.com/s/article/83260

Cách 2: Trong trường hợp không thể cài đặt bản vá hoặc không có bản vá cho phiên bản vRealize Operations đang sử dụng, quản trị viên có thể thực hiện biện pháp khắc phục thay thế bằng cách xóa dòng cấu hình khỏi file casa-security-context.xml như sau:

Bước 1: Đăng nhập vào Primary node với quyền root thông qua SSH hoặc Console (nhấn ALT+F1 trong Console để đăng nhập)

Bước 2: Mở file

/user/lib/vmware-case-webapps/case/WEB-INF/classes/spring/casa-security-context.xml trong trình soạn thảo.

Bước 3: Tìm và xóa dòng:

```
<sec:http pattern="/nodes/thumbprints" security='none'/>
```

Bước 4: Lưu và đóng file.

Bước 5: Khởi động lại dịch vụ CaSA:

```
service vmware-casa restart
```

Bước 6: Thực hiện lại các bước từ 1-5 trên tất cả các nodes khác trên vRealize Operations custer.

3. Nguồn tin tham khảo

https://www.vmware.com/security/advisories/VMSA-2021-0004.html

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn 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