

Số: /TTCNTT-KTHT  
V/v 19 lỗ hổng bảo mật mới trong VMware

Hà Nội, ngày tháng năm 2021

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

Ngày 21/9/2021 vừa qua, VMware vừa công bố 19 lỗ hổng bảo mật ảnh hưởng đến VMware vCenter Server phiên bản 7.0/6.7/6.5 và VMware vCloud Foundation phiên bản 4.3.1/3.10.2.2. Trong đó đáng chú ý:

- Lỗ hổng bảo mật (**CVE-2021-22005**) có mức ảnh hưởng nghiêm trọng (điểm CVSS: 9.8), cho phép đối tượng tấn công không cần xác thực có thể thực thi mã tùy ý.

- 11 lỗ hổng bảo mật (CVE-2021-21991, CVE-2021-22006, CVE-2021-22011, CVE-2021-22015, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22014, CVE-2021-22018, CVE-2021-21992) có mức ảnh hưởng cao, cho phép đối tượng tấn công khai thác dưới nhiều hình thức khác nhau như thu thập thông tin, tấn công leo thang, tấn công từ chối dịch vụ,... Trong đó có **07** lỗ hổng bảo mật (**CVE-2021-22006, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018**) có thể khai thác mà không cần xác thực.

Thông tin chi tiết các lỗ hổng có tại Phụ lục kèm theo.

Các sản phẩm của VMware được sử dụng khá phổ biến trong các cơ quan tổ chức, doanh nghiệp; đã và đang là mục tiêu nhắm đến của các đối tượng tấn công mạng; đặc biệt là các nhóm chuyên thực hiện tấn công APT.

Trung tâm Công nghệ thông tin cũng đã có cảnh báo về các lỗ hổng bảo mật trước đây liên quan đến sản phẩm VMware. Vì vậy, việc thường xuyên kiểm tra, rà soát hệ thống thông tin của các cơ quan tổ chức để xử lý và khắc phục các lỗ hổng bảo mật đang tồn tại trong hệ thống là hết sức cần thiết.

Nhằm đảm bảo 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. Thực hiện cập nhật bản vá phù hợp với phiên bản sản phẩm VMware đang sử dụng.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần thiết, Quý đơn vị 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 (đề b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

**GIÁM ĐỐC**

**Hà Quốc Trung**

**Phụ lục**  
**Thông tin lỗ hổng bảo mật**  
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021  
của Trung tâm Công nghệ thông tin)

**1. Thông tin về các lỗ hổng**

STT	CVE	Mô tả
1	CVE-2021-22005	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenter Server, cho phép đối tượng tấn công không cần xác thực thực thi mã tùy ý. - Điểm CVSS: 9.8 (ngghiêm trọng)
2	CVE-2021-21991	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công đã xác thực thực hiện tấn công leo thang. - Điểm CVSS: 8.8 (cao)
3	CVE-2021-22006	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực bypass proxy, truy cập trái phép. - Điểm CVSS: 8.3 (cao)
4	CVE-2021-22011	- Lỗ hổng trong vCenter Server Content Library, cho phép đối tượng tấn công không cần xác thực truy cập một số API. - Điểm CVSS: 8.1 (cao)
5	CVE-2021-22015	- Lỗ hổng trong vCenter Server Content Library, cho phép đối tượng tấn công đã xác thực thực hiện tấn công leo thang. - Điểm CVSS: 7.8 (cao)
6	CVE-2021-22012	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực truy cập một số API và thu thập thông tin. - Điểm CVSS: 7.5 (cao)
7	CVE-2021-22013	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thu thập thông tin từ một số API. - Điểm CVSS: 7.5 (cao)
8	CVE-2021-22016	- Lỗ hổng trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công XSS. - Điểm CVSS: 7.5 (cao)
9	CVE-2021-22017	- Lỗ hổng tồn tại trong vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công XSS.

		- Điểm CVSS: 7.3 (cao)
10	CVE-2021-22014	- Lỗ hổng tồn tại trong VAMI (Virtual Appliance Management Infrastructure), cho phép đối tượng có quyền cao trên hệ thống thực hiện tấn công thực thi mã tùy ý. - Điểm CVSS: 7.2 (cao)
11	CVE-2021-22018	- Lỗ hổng tồn tại trong VMware vSphere Life cycle Manager plug-in, cho phép đối tượng tấn công không cần xác thực thực hiện xóa tệp tùy ý. - Điểm CVSS: 6.5 (cao)
12	CVE-2021-21992	- Lỗ hổng tồn tại trong quá trình xử lý XML của vCenter Server, cho phép đối tượng tấn công đã xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 6.5 (cao)
13	CVE-2021-22007	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenter Server, cho phép đối tượng tấn công đã xác thực thu thập thông tin nội bộ của máy chủ. - Điểm CVSS: 5.5 (trung bình)
14	CVE-2021-22019	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenterServer, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
15	CVE-2021-22009	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
16	CVE-2021-22010	- Lỗ hổng tồn tại trong dịch vụ VPXD (Virtual Provisioning X Daemon) của vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công từ chối dịch vụ. - Điểm CVSS: 5.3 (trung bình)
17	CVE-2021-22008	- Lỗ hổng tồn tại trong dịch vụ VAPI (vCenter API) của vCenter Server, cho phép đối tượng tấn công không cần xác thực thực hiện tấn công thu thập thông tin. - Điểm CVSS: 5.3 (trung bình)
18	CVE-2021-22020	- Lỗ hổng tồn tại trong dịch vụ Analytics của vCenterServer, cho phép đối tượng tấn công đã xác thực thực hiện tấn công từ chối dịch vụ.

		- Điểm CVSS: 5.0 (trung bình)
19	CVE-2021-21993	- Lỗ hổng tồn tại trong vCenter Server Content Library, cho phép đối tượng tấn công đã xác thực thực hiện tấn công SSRF. - Điểm CVSS: 4.3 (trung bình)

- **Ảnh hưởng:** vCenter Server phiên bản 7.0/6.7/6.5 và vCloud Foundation phiên bản 4.3.1/3.10.2.2.

## 2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Thông tin các bản vá tham khảo tại: <https://www.vmware.com/security/advisories/VMSA-2021-0020.html>

## 3. Nguồn tham khảo

<https://www.vmware.com/security/advisories/VMSA-2021-0020.html>

**DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT**  
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm  
Công nghệ thông tin)

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