UBND TỈNH AN GIANG **SỞ Y TẾ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do – Hạnh phúc**
Số: 3191/ SYT-NVY V/v lỗ hổng bảo mật nghiêm trọng trong Camera IP Hikvision và 19 lỗ hổng bảo mật mới trong VMware	*An Giang, ngày 05 tháng 10 năm 2021*

Kính gửi:

- Các Bệnh viện tuyến tỉnh công lập và tư nhân;
- Trung tâm Y tế huyện, thành phố.

Căn cứ Công văn số 736/CNTT-YTĐT ngày 30 tháng 9 năm 2021 của Cục Công nghệ thông tin Bộ Y tế về việc 19 lỗ hổng bảo mật mới trong VMware;

Căn cứ Công văn số 737/CNTT-YTĐT ngày 30 tháng 9 năm 2021 của Cục Công nghệ thông tin Bộ Y tế về việc lỗ hổng nghiêm trọng trong Camera IP Hikvision;

Căn cứ Công văn số 1092/CV-ĐƯCKCSCATTTM ngày 30 tháng 9 năm 2021 của Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh An Giang về việc lỗ hổng bảo mật nghiêm trọng trong Camera IP Hikvision và 19 lỗ hổng bảo mật mới trong VMware;

Trên cơ sở thực tế triển khai công tác giám sát an toàn thông tin trong thời gian gần đây, theo phân tích và đánh giá từ Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) - Cục An toàn thông tin có khả năng mã khai thác của các lỗ hổng sẽ sớm được công khai trên Internet trong thời gian sắp tới. 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. Cụ thể các lỗ hổng bảo mật như sau:

a. Hikvision vừa công bố bảo mật **CVE-2021-36260** trong sản phẩm Camera IP. Lỗ hổng này có điểm CVSS:9.8 (nghiêm trọng), cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực, từ đó chiếm toàn quyền kiểm soát thiết bị, thông qua đó có thể truy cập và tấn công mạng nội bộ của cơ quan, tổ chức; lỗ hổng này ảnh hưởng khá lớn và có thể gây rủi ro cho các cơ sở hạ tầng quan trọng. *(Thông tin tại phụ lục kèm theo)*

b. Trong các sản phẩm của VMware có công bố 19 lỗ hổng bảo mật ảnh hưởng đến **VMware vCenter Server** phiên bản 7.0/6.7/6.5 và **VMware vClound Foundation** phiên bản 4.3.1/3.10.2.2. 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 nhằm đến của các đối tượng tấn công mạng; đặc biệt là các nhóm chuyên thực hiện tấn công APT. *(Thông tin tại phụ lục kèm theo)*.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin y tế của các đơn vị góp phần bảo đảm an toàn cho không gian mạng, Sở Y tế khuyến nghị các Bệnh viện tuyến tỉnh, Trung tâm Y tế các huyện, thị xã, thành phố thực hiện:

1. Kiểm tra, rà soát và xác định hệ thống thông tin có sử dụng và những hệ thống thông tin có kết nối với thiết bị Camera IP Hikvision; nếu sử dụng cần thực hiện cập nhật firmware, tách riêng dải mạng dùng cho camera và hạn chế truy cập đến các dải mạng khác.

2. 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.

3. 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.

Trân trọng./.

Nơi nhận :
- Như trên;
- Lưu: VT, NVY.

(đính kèm phụ lục)

GIÁM ĐỐC

Trần Quang Hiền

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số / SYT-NVY ngày 04/10/2021 của Sở Y tế)

1. Thông tin lỗ hổng bảo mật CVE-2021-36260 (Camera IP Hikvision)

- **Mô tả**: Lỗ hổng ảnh hưởng đến sản phẩm camera IP Hikvision, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực, từ đó chiếm toàn quyền kiểm soát thiết bị và có thể truy cập và tấn công mạng nội bộ của mục tiêu.

- **Điểm CVSS**: 9.8 (nghiêm trọng)

- **Ảnh hưởng:**

Tên sản phẩm	Phiên bản ảnh hưởng
DS-2CVxxx1 DS-2CVxxx5 DS-2CVxxx6	Versions which Build time before 210625
HWI-xxxx	
IPC-xxxx	
DS-2CD1xx1	
DS-2CD1x23 DS-2CD1x43(B) DS-2CD1x43(C) DS-2CD1x43G0E DS-2CD1x53(B) DS-2CD1x53(C)	
DS-2CD1xx7G0	
DS-2CD2xx6G2 DS-2CD2xx7G2	
DS-2CD2xx2WD	
DS-2CD2x21G0	
DS-2CD2xx3G2	
DS-2CD3xx6G2 DS-2CD3xx7G2	
DS-2CD3xx7G0E	
DS-2CD3x21G0 DS-2CD3x51G0	
DS-2CD3xx3G2	
DS-2CD4xx0 DS-2CD4xx6 DS-2CD5xx7 DS-2CD5xx5 iDS-2XM6810	

iDS-2CD6810	
DS-2XE62x7FWD (D) DS-2XE30x6FWD (B) DS-2XE60x6FWD (B) DS-2XE62x2F (D) DS-2XC66x5G0 DS-2XE64x2F (B)	
DS-2CD7xx6G0 DS-2CD8Cx6G0	
KBA18 (C) -83x6FWD	
(i) DS-2DExxxx	
(i) DS-2PTxxxx	
(i) DS-2SE7xxxx	
DS-2DYHxxxx	
DS-DY9xxxx	
PTZ-Nxxxx	
HWP-Nxxxx	
DS-2DF5xxxx DS-2DF6xxxx DS-2DF6xxxx-Cx DS-2DF7xxxx DS-2DF8xxxx DS-2DF9xxxx	
iDS-2PT9xxxx	
iDS-2SK7xxxx iDS-2SK8xxxx	
iDS-2SR8xxxx	
iDS-2VSxxxx	
DS-2TBxxx DS-Bxxxx DS-2TDxxxxB	Versions which Build time before 210702
DS-2TD1xxx-xx DS-2TD2xxx-xx	
DS-2TD41xx-xx / Wx DS-2TD62xx-xx / Wx DS-2TD81xx-xx / Wx	

DS-2TD4xxx-xx / V2 DS-2TD62xx-xx / V2 DS-2TD81xx-xx / V2	
DS-76xxNI-K1xx DS-76xxNI-Qxx DS-HiLookI-NVR-1xxMHxx DS-HiLookI-NVR-2xxMHxx DS-HiWatchI-HWN-41xxMHxx DS-HiWatchI-HWN-42xxMHxx	V4.30.210 Build201224 - V4.31.000 Build210511
DS-71xxNI-Q1xx DS-HiLookI-NVR-1xxMHxx DS-HiLookI-NVR-1xxHxx DS-HiWatchI-HWN-21xxMHxx DS-HiWatchI-HWN-21xxHxx	V4.30.300 Build210221 - V4.31.100 Build210511

2. Thông tin lỗ hổng bảo mật trong VMware

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

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 (nghiêm 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 vCenterServer, 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 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)
16	CVE-2021-22010	- Lỗ hổng tồn tại trong dịch vụ VPXD (Virtual Provisioning X Daemon) 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)
17	CVE-2021-22008	- 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 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)

3. Hướng dẫn khắc phục

a. Lỗ hổng bảo mật CVE-2021-36260 (Camera IP Hikvision)

Để khắc phục lỗ hổng bảo mật nói trên, người dùng nên tải bản cập nhật firmware phù hợp với sản phẩm đang sử dụng, tách riêng dải mạng dùng cho Camera IP, hạn chế truy cập đến các dải mạng khác.

Thông tin các bản cập nhật firmware có tại:

https://www.hikvision.com/en/support/download/firmware

b. Lỗ hổng bảo mật trong VMware

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

4. Nguồn tham khảo

https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products

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