UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 8602 /STNMT - CNTT
V/v cảnh báo các lỗ hổng bảo mật ảnh hưởng đến phần mềm VMware và thiết bị Camera IP.

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

Thanh Hoá, ngày 04 tháng10 năm 2021

Kính gửi: Trưởng các đơn vị thuộc Sở.

Sở Tài nguyên và Môi trường nhận được Công văn số 2028/STTTT&CNTT ngày 28/9/2021 của Sở Thông tin và Truyền thông về việc cảnh báo các lỗ hổng bảo mật mới ảnh hưởng đến phần mềm VMware và thiết bị Camera IP.

Trong thời gian gần đây, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận các điểm yếu, lỗ hổng bảo mật mới trên các phần mềm, ứng dụng đang được sử dụng rộng rãi trong các hệ thống thông tin của các cơ quan, tổ chức và doanh nghiệp. Trong đó, có những lỗ hổng bảo mật mức cao và nghiêm trọng có thể bị khai thác, sử dụng để tấn công có chủ đích trong diện rộng. Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại hệ thống thông tin của Sở. Giám đốc Sở yêu cầu các đơn vị thuộc Sở khẩn trương triển khai một số nội dung sau:

1. Giao Trung tâm Công nghệ thông tin:

- Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; hỗ trợ các đơn vị khi có khó khăn vướng mắc.

- Đăng tải toàn bộ nội dung Công văn số 2028/STTTT&CNTT ngày 28/9/2021 của Sở Thông tin và Truyền thông trên Cổng thông tin điện tử Sở Tài nguyên và Môi trường Thanh Hóa.

2. Giao trưởng các đơn vị thuộc Sở:

- Phổ biến, quán triệt đến toàn thể công chức, viên chức và người lao động thuộc đơn vị mình thực hiện kiểm tra, rà soát và xác định các máy tính, máy chủ

đang cài đặt các phần mềm, ứng dụng có khả năng bị ảnh hưởng bởi các lỗ hổng trên, liên hệ với Trung tâm Công nghệ thông tin để có phương án xử lý, khắc phục lỗ hổng. Cập nhật phiên bản mới nhất theo khuyến nghị của hãng sản xuất để khắc phục các nguy cơ mất an toàn thông tin. *(Có phụ lục thông tin các lỗ hổng bảo mật kèm theo).*

Theo các nội dung trên, yêu cầu Trưởng các đơn vị quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/c);
- Lưu: VT, TTCNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH THANH HÓA

Phùng Đình Ảnh

Phụ lục: Thông tin các lỗ hổng bảo mật
(Kèm theo công văn số /STNMT-CNTT ngày tháng năm 2021 của Sở Tài nguyên và Môi trường)

1. Thông tin lỗ hổng bảo mật sản phẩm Vmware

Sản phẩm ảnh hưởng: vCenter Server phiên bản 7.0/6.7/6.5 và vCloud 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 Lifecycle 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)

2. Thông tin lỗ hổng bảo mật sản phẩm Camera IP

Tên sản phẩm	Phiên bản ảnh hưởng
DS-2CVxxx1	Versions which Build time before 210625

DS-2CVxxx5 DS-2CVxxx6	
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-HWN41xxMHxx DS-HiWatchI-HWN42xxMHxx	V4.30.210 Build201224 - V4.31.000 Build210511
DS-71xxNI-Q1xx DS-HiLookI-NVR-1xxMHxx DS-HiLookI-NVR-1xxHxx DS-HiWatchI-HWN21xxMHxx DS-HiWatchI-HWN-21xxHxx	V4.30.300 Build210221 - V4.31.100 Build210511