UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1741 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật nghiêm trọng trong Camera IP Hikvision, VMware và các sản phẩm của Microsoft.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Tây Ninh, ngày 21 tháng 10 năm 2021

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành tỉnh;
- UBND các huyện, thị xã, thành phố
- Viễn thông Tây Ninh;
- Viettel Tây Ninh.

Thực hiện theo công văn số **1287/CATTT-NCSC**, **1286/CATTT-NCSC** và **1411/CATTT-NCSC** của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật bảo mật nghiêm trọng trong Camera IP Hikvision (**CVE-2021-36260**), 19 lỗ hổng VMware (**CVE-2021-22005, CVE-2021-21991, CVE-2021-22006, CVE-2021-22011, CVE-2021-22015….)** và các lỗ hổng bảo mật trong các sản phẩm của Microsoft.

Để đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Rà soát, kiểm tra cho các máy tính/máy chủ/thiết bị nếu nằm trong phạm vi ảnh hưởng của lỗ hổng bảo mật và tiến hành khắc phục *(Phụ lục hướng dẫn kèm theo)*.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

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

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC I
HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG BẢO MẬT CAMERA IP HIKVISION

1. Thông tin lỗ hổng bảo mật

- 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 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)	Versions which Build time before 210625

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 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	Versions which Build time before 210702
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

- **Đánh giá mức độ:** giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến hơn 100 triệu thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng mã khai thác của lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

2. Hướng dẫn khắc phục: 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

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

PHỤ LỤC II
HƯỚNG DẪN KHẮC PHỤC 19 LỖ HỔNG BẢO MẬT MỚI TRONG VMWARE

1. Thông tin lỗ hổng bảo mật

- Mô tả: 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

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)

- Ảnh hưởng đến: vCenter Server phiên bản 7.0/6.7/6.5 và vClound 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

PHỤ LỤC III
HƯỚNG DẪN KHẮC PHỤC CÁC LỖ HỔNG BẢO MẬT TRONG CÁC SẢN PHẨM MICROSOFT

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2021-26427	- CVSS: 9.0 (cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26427
2	CVE-2021-41344 CVE-2021-40487	- CVSS: 8.1 (cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40487 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41344
3	CVE-2021-40469	- CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469
4	CVE-2021-40486	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40486
5	CVE-2021-38672 CVE-2021-40461	- CVSS: 8.0 (cao) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38672 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40461
6	CVE-2021-40471 CVE-2021-40473 CVE-2021-40374	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40471 https://msrc.microsoft.com/up

	CVE-2021-40479 CVE-2021-40485	công thực thi mã từ xa	date-guide/vulnerability/CVE-2021-40473 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40474 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40479 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40485
7	CVE-2021-40480 CVE-2021-40481	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40480 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40481
8	CVE-2021-41330	- CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Windows Media Foundation cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41330
9	CVE-2021-41342	- CVSS: 6.8 (cao) - Lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực thi mã từ xa	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41342

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. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu thm khảo: https://msrc.microsoft.com/update-guide/en-us