BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOAN THÔNG TIN

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

Số: 1287/CATTT-NCSC
V/v lỗ hổng bảo mật nghiêm trọng trong Camera IP Hikvision

Hà Nội, ngày 22 tháng 09 năm 2021

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 19/9/2021 vừa qua, Hikvision vừa công bố lỗ hổng 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.

Camera IP được các cơ quan tổ chức, doanh nghiệp sử dụng khá phổ biến hiện nay vì vậy lỗ hổng này ảnh hưởng khá lớn và có thể gây rủi ro cho các cơ sở hạ tầng quan trọng. Theo đánh 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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị 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. 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 hỗ trợ, Quý đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục

Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

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	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	V4.30.210 Build201224 - V4.31.000 Build210511

DS-HiLookI-NVR-2xxMHxx DS-HiWatchI-HWN-41xxMHxx DS-HiWatchI-HWN-42xxMHxx	
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. 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 firware 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