Logo
Logo not found or type unknown

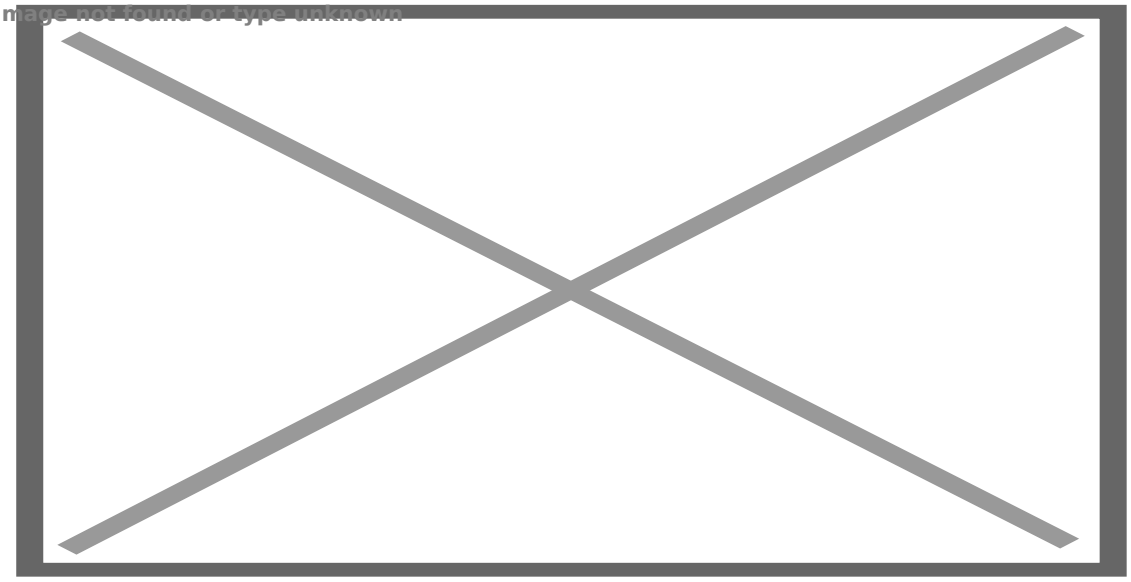
Lỗ hổng nguy hiểm trong camera Hikvision tại Việt Nam

20:18 27/09/2021

Tác giả: Thế Anh

Cục An toàn thông tin (Bộ Thông tin và Truyền thông) vừa có cảnh báo về lỗ hổng nghiêm trọng trong sản phẩm camera IP của Hikvision. Lỗ hổng này được nhận định ảnh hưởng đến hơn 100 triệu thiết bị trên toàn cầu trong đó có cả Việt Nam.

Image not found or type unknown



Cảnh báo về lỗ hổng bảo mật trong camera IP.

Trong thông tin cảnh báo về lỗ hổng bảo mật nghiêm trọng trong camera IP Hikvision gửi tới các đơn vị chuyên trách về công nghệ thông tin (CNTT) các bộ, ngành, địa phương; các tập đoàn, tổng công ty nhà nước; các ngân hàng, tổ chức tổ chức tài chính và hệ thống các đơn vị chuyên trách về an toàn thông tin hôm nay, ngày 22/9, Cục An toàn thông tin cho biết, hãng Hikvision vừa công bố lỗ hổng bảo mật CVE-2021-36260 trong sản phẩm camera IP.

Được các chuyên gia nhận định là lỗ hổng nghiêm trọng, lỗ hổng CVE-2021-36260 trong camera 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, thông qua đó có thể truy cập và tấn công mạng nội bộ của cơ quan, tổ chức.

Hiện nay, camera IP được các cơ quan, tổ chức, doanh nghiệp sử dụng khá phổ biến. Theo đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng CVE-2021-36260 ảnh hưởng đến hơn 100 triệu thiết bị trên toàn cầu trong đó có cả Việt Nam. Vì thế, lỗ hổng này ảnh hưởng khá lớn và có thể gây rủi

ro cho các cơ sở hạ tầng quan trọng.

Đáng chú ý, Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin đánh giá: Khả năng mã khai thác của lỗ hổng bảo mật CVE-2021-36260 sẽ sớm được công khai trên Internet trong thời gian sắp tới.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của đơn vị, góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị các cơ quan, tổ chức, doanh nghiệp 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 có sử dụng, đơn vị cần thực hiện cập nhật phần mềm, tách riêng dải mạng dùng cho camera và hạn chế truy cập đến các dải mạng khác.

Các cơ quan, đơn vị, doanh nghiệp cũng được khuyến nghị 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, các cơ quan, đơn vị, doanh nghiệp liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Đối với các doanh nghiệp đang sử dụng thiết bị IP của Hikvision, nguy cơ là doanh nghiệp có thể bị lộ thông tin hình ảnh, nguy hiểm hơn là những thiết bị này có thể bị tấn công và trở thành một máy tính trong mạng và có thể tấn công nội bộ hoặc có thể biến thiết bị này thành những máy chủ ma dùng cho các mục đích xấu. Do đó, nếu đã lắp camera không an toàn, nên cách ly và thực hiện cập nhật phiên bản vá lỗi. Đối với các thiết bị chưa có bản vá lỗi chỉ nên sử dụng dạng camera qua đầu ghi, tránh sử dụng tính năng camera qua Internet.

Theo baotintuc

Link bài viết: https://nguoilambao.vn/lo-hong-nguy-hiem-trong-camera-hikvision-tai-viet-nam