BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 724 /QĐ-BTTTT

Hà Nội, ngày 07 tháng 5 năm 2024

QUYẾT ĐỊNH

Ban hành Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26 tháng 07 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Chỉ thị số 23/CT-TTg ngày 26 tháng 12 năm 2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Bộ tiêu chí về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thủ tướng Chính phủ (để b/c);
- Phó TTgCP Trần Lưu Quang (để b/c);
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long;
- Đơn vị chuyên trách về CNTT/ATTT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Toàn án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam; Kiểm toán Nhà nước;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cổng Thông tin điện tử Bộ TT&TT (để đăng tải);
- Lưu: VT, CATTT.ATHTTT.NMD.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Phạm Đức Long

BỘ THÔNG TIN VÀ TRUYỀN THÔNG **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Độc lập - Tự do - Hạnh phúc

BỘ TIÊU CHÍ VỀ YÊU CẦU AN TOÀN THÔNG TIN MẠNG CƠ BẢN CHO CAMERA GIÁM SÁT

(Kèm theo Quyết định số /QĐ-BTTTT ngày tháng 5 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi điều chỉnh

Tài liệu này đưa ra và khuyến nghị áp dụng các yêu cầu kỹ thuật an toàn thông tin mạng cơ bản cho thiết bị camera giám sát sử dụng giao thức mạng (gọi tắt là thiết bị camera).

Đối với các yêu cầu kỹ thuật an toàn thông tin mạng ở mức cao hơn, các tổ chức, cá nhân căn cứ đặc thù, nhu cầu thực tiễn của mình để xem xét, quyết định.

2. Đối tượng áp dụng

Khuyến nghị áp dụng đối với các tổ chức, cá nhân Việt Nam và nước ngoài có liên quan đến hoạt động nghiên cứu, phát triển, sản xuất, đánh giá, lựa chọn và sử dụng thiết bị camera.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau:

3.1. Dịch vụ liên kết (Associated services)

Các thành phần liên quan (ứng dụng, thiết bị kỹ thuật số, công nghệ thông tin) cung cấp các chức năng phục vụ hoạt động của thiết bị camera.

Ví dụ: Ứng dụng di động; hệ thống điện toán, lưu trữ đám mây; giao diện lập trình ứng dụng (API) của bên thứ ba...

3.2. Chế độ cài đặt gốc (Factory default)

Trạng thái hoạt động của thiết bị camera bao gồm thông số, tùy chọn, chức năng đã được khởi tạo, thiết lập mặc định trước theo thiết kế của nhà sản xuất. Chế độ này được kích hoạt ngay sau khi thiết bị camera được lắp đặt và khởi động lần đầu tiên.

3.3. Chức năng cảm biến (Sensing capability)

Chức năng của thiết bị camera cho phép thu thập dữ liệu về môi trường xung quanh.

Ví dụ: Dữ liệu hình ảnh; dữ liệu âm thanh; dữ liệu sinh trắc học; dữ liệu vị trí;...

3.4. Gỡ lỗi (Debug)

Việc thực hiện các thao tác và lệnh giao tiếp với thiết bị camera để phát triển chức năng hoặc tìm ra các lỗi của thiết bị.

3.5. Giao diện gỡ lỗi (Debug interface)

Giao diện vật lý của thiết bị camera được sử dụng để thực hiện chức năng gỡ lỗi.

3.6. Giao diện logic (Logical interface)

Giao diện của thiết bị camera cho phép kết nối, quản trị thiết bị camera thông qua kết nối mạng.

3.7. Giao diện mạng (Network interface)

Giao diện vật lý của thiết bị camera được sử dụng để truy cập vào các chức năng của thiết bị thông qua kết nối mạng.

3.8. Giao diện vật lý (Physical interface)

Cổng vật lý hoặc giao diện kết nối vô tuyến của thiết bị camera cho phép giao tiếp với thiết bị camera thông qua kết nối vật lý.

Ví dụ: Cổng Ethernet; cổng USB; Wifi;...

3.9. Mật khẩu khởi tạo (Initial password)

Mật khẩu được thiết lập khi người sử dụng truy cập lần đầu tiên vào thiết bị.

3.10. Mật khẩu mặc định (Default password)

Mật khẩu được thiết lập mặc định khi thiết bị được sản xuất.

3.11. Quá trình khởi động (Initialization)

Quá trình thiết lập kết nối mạng và các thông số liên quan cho thiết bị camera để vận hành.

3.12. Thông số bảo mật bí mật (Private security parameter)

Các thông tin bí mật của thiết bị camera dùng để bảo vệ thông tin hoặc quản lý truy cập, cấu hình thiết bị.

Ví dụ: Mật khẩu; mã PIN; khóa mật mã bí mật; phần nội dung bí mật của chứng chỉ số;...

3.13. Thông số bảo mật công khai (Public security parameter)

Các thông tin công khai của thiết bị camera có thể cung cấp để phục vụ kết nối, quản trị và sử dụng thiết bị camera.

Ví dụ: Khóa mật mã công khai; phần nội dung công khai của chứng chỉ số;...

3.14. Thông số bảo mật nhạy cảm (Sensitive security parameter)

Thông số bảo mật thuộc một trong hai loại là thông số bảo mật bí mật và thông số bảo mật công khai.

3.15. Trạng thái hoạt động ban đầu (Initialized state)

Trạng thái hoạt động của thiết bị camera ngay sau quá trình khởi động, bao gồm các thông số, tùy chọn, chức năng đã được khởi tạo, thiết lập, kích hoạt trong quá trình khởi động.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

Có tài liệu hướng dẫn sử dụng sản phẩm cho người sử dụng.

2. Quản lý xác thực

2.1. Phòng chống tấn công vét cạn

a) Có chức năng quản trị hệ thống cho phép thay đổi thời gian khóa, số lần đăng nhập sai và khoảng thời gian đăng nhập sai liên tục; Thiết lập mặc định khóa không cho đăng nhập trong vòng 5 phút, sau khi đăng nhập thất bại 5 lần liên tục trong khoảng thời gian 30 giây hoặc ngắn hơn.

b) Chỉ thông tin cho người sử dụng nội dung đăng nhập thành công/thất bại mà không có nội dung khác làm cơ sở thực hiện tấn công vét cạn.

2.2. Quản lý mật khẩu an toàn

a) Có chức năng yêu cầu người dùng bắt buộc thay đổi mật khẩu mặc định hoặc mật khẩu khởi tạo khi sử dụng thiết bị lần đầu tiên.

b) Có chức năng kiểm soát mật khẩu an toàn. Mật khẩu được tạo ra phải có yêu cầu về độ phức tạp đối với mật khẩu (mật khẩu phải có độ dài tối thiểu 8 ký tự, có chữ hoa, chữ thường, chữ số, ký tự đặc biệt).

c) Sử dụng hàm băm SHA-256 hoặc cao hơn.

2.3. Khởi tạo mật khẩu mặc định an toàn

Mật khẩu khởi tạo mặc định trên thiết bị camera và các dịch vụ liên kết (nếu có) phải đáp ứng các yêu cầu sau:

a) Có độ dài tối thiểu 8 ký tự, có chữ hoa, chữ thường, chữ số, ký tự đặc biệt.

b) Cơ chế khởi tạo mật khẩu sử dụng phương pháp sinh mã có giá trị ngẫu nhiên.

c) Cơ chế khởi tạo mật khẩu không dùng các thông tin công khai (ví dụ: địa chỉ MAC; chuỗi định danh Wifi SSID; tên sản phẩm; loại sản phẩm;...).

d) Là khác nhau đối với mỗi thiết bị camera khác nhau.

2.4. Quản lý xác thực

a) Có chức năng xác thực cho phép xác thực nhiều loại đối tượng khác nhau như người dùng hoặc thiết bị với thiết bị với loại giá trị xác thực khác nhau.

b) Mật khẩu lưu trữ trên camera phải được mã hóa.

3. Quản lý lỗ hổng bảo mật

3.1. Yêu cầu đối với hệ thống quản lý lỗ hổng của thiết bị

Nhà sản xuất có hệ thống trực tuyến cho phép tiếp nhận và công bố thông tin về lỗ hổng của thiết bị tới người sử dụng.

3.2. Yêu cầu đối với thông tin công bố lỗ hổng bảo mật của thiết bị

a) Có mô tả về lỗ hổng, phân loại và xác định mức độ nghiêm trọng;

b) Có mô tả về các phiên bản bị ảnh hưởng.

c) Có hướng dẫn cập nhật, xử lý lỗ hổng.

4. Quản lý và thực hiện cập nhật

4.1. Yêu cầu đối với hệ thống quản lý cập nhật

Nhà sản xuất có hệ thống trực tuyến cho phép:

a) Công bố thông tin về các phiên bản cập nhật.

b) Quản lý và thực hiện cập nhật đối với các thiết bị camera có chức năng kết nối Internet.

4.2. Yêu cầu đối với thông tin của phiên bản cập nhật

Thông tin phiên bản cập nhật bao gồm tối thiểu các thông tin:

a) Phiên bản phần mềm hệ thống.

b) Mã kiểm tra an toàn đối với phần mềm hệ thống.

c) Có mô tả về thông tin phần mềm hệ thống được cập nhật.

4.3. Yêu cầu đối với chức năng cập nhật phiên bản qua Internet

a) Chức năng cập nhật phải được thực hiện qua kênh kết nối mạng an toàn có phương pháp mã hóa an toàn đáp ứng yêu cầu tại Mục 6.1 tài liệu này.

b) Có chức năng xác thực trước khi thực hiện cập nhật.

c) Có chức năng thông báo khi có phiên bản cập nhật mới khi người dùng đăng nhập, quản trị thiết bị.

d) Có chức năng thiết lập cho phép thiết bị tự động cập nhật bản vá từ nhà sản xuất.

đ) Có chức năng kiểm tra tính nguyên vẹn của bản cập nhật có sử dụng chữ

ký số của nhà sản xuất.

5. Quản lý phiên an toàn

5.1. Quản lý phiên đăng nhập

Thiết bị camera, ứng dụng giao tiếp với người sử dụng có chức năng lựa chọn timeout cho phép tự động đăng xuất ứng dụng sau một khoảng thời gian.

5.2. Tạo khóa phiên an toàn

Tạo khóa phiên cho người sử dụng khi đăng nhập thành công đáp ứng các yêu cầu sau:

a) Khóa phiên không có khả năng bị tấn công vét cạn.

b) Khóa phiên không được sinh cố định, có yếu tố ngẫu nhiên.

c) Khóa phiên không có khả năng bị khôi phục:

d) Có chức năng yêu cầu hủy phiên đăng nhập hoặc hủy phiên đăng nhập cũ khi người dùng đăng nhập lại.

6. Quản lý kênh giao tiếp

6.1. Yêu cầu đối với các giao tiếp kết nối an toàn

a) Sử dụng các phương pháp mã hóa dựa trên các tiêu chuẩn Việt Nam hiện hành hoặc tiêu chuẩn quốc tế tương đương.

b) Phương pháp mã hóa sử dụng phiên bản không tồn tại lỗ hổng, điểm yếu an toàn thông tin mạng được công bố bởi các cơ quan, tổ chức trong nước hoặc nước ngoài.

6.2. Truy cập cấu hình thiết bị an toàn

a) Sử dụng kênh bảo mật an toàn trước khi thực hiện truy cập, cấu hình thiết bị.

b) Kiểm soát truy cập cấu hình thiết bị:

i. Cấp quyền truy cập tối thiểu (chỉ phục vụ việc cấu hình và quản trị thiết bị) với đối tượng xác thực thành công.

ii. Không cấp quyền truy cập đối với đối tượng xác thực thất bại.

iii. Không cấp quyền truy cập đối với đối tượng chưa xác thực.

c) Từ chối đối tượng xác thực (người và máy) truy cập khi camera ở trạng thái hoạt động ban đầu đối với:

i. Đối tượng xác thực thành công nhưng không có đủ quyền truy cập.

ii. Đối tượng xác thực thất bại.

iii. Đối tượng chưa xác thực.

Ngoại lệ: Tất cả yêu cầu trên không áp dụng đối với các dịch vụ hệ thống, phục vụ hoạt động của thiết bị camera như: ARP; DHCP; DNS; ICMP; NTP;...

7. Quản lý giao diện

7.1. Bảo mật thông tin xác thực

Ở trạng thái hoạt động ban đầu, khi người sử dụng chưa được xác thực, giao diện mạng của thiết bị chỉ cung cấp các thông tin công khai liên quan đến vận hành và sử dụng thiết bị.

7.2. Quản lý giao diện logic và mạng

a) Các giao diện logic và mạng được kích hoạt khi thiết bị ở trạng thái hoạt động ban đầu phải có mô tả mục đích sử dụng, để giải thích tại sao giao diện được kích hoạt.

b) Có chức năng cho phép kích hoạt hoặc vô hiệu hóa giao diện theo mô tả.

7.3. Quản lý giao diện gỡ lỗi

Giao diện gỡ lỗi phải được mặc định vô hiệu hóa.

7.4. Quản lý giao diện vật lý

a) Có chức năng vô hiệu hóa các cổng kết nối vật lý khi không sử dụng.

b) Tất cả giao diện vật lý mà không sử dụng phải được vô hiệu hóa truy cập ở chế độ cài đặt gốc.

8. Bảo đảm an toàn thông tin dữ liệu người sử dụng

8.1. Bảo vệ dữ liệu cá nhân

Thiết bị camera và các dịch vụ liên kết có tối thiểu tính năng cho phép thiết lập, cấu hình địa điểm tại Việt Nam đối với việc xử lý, lưu trữ và khai thác dữ liệu (như: trên thẻ nhớ/thiết bị ngoại vi, dịch vụ điện toán đám mây đặt tại Việt Nam,...) nhằm đảm bảo tuân thủ quy định của pháp luật Việt Nam về bảo vệ dữ liệu cá nhân.

8.2. Cảm biến thu thập dữ liệu

Tài liệu hướng dẫn sử dụng (hoặc tài liệu tương đương được công bố công khai) phải liệt kê danh mục các cảm biến được sử dụng bởi thiết bị camera và mô tả chức năng, nguyên lý hoạt động của từng cảm biến được thiết bị camera sử dụng.

8.3. Thông báo liên quan đến bảo vệ dữ liệu cá nhân

Trong quá trình khởi tạo, thiết lập, cấu hình thiết bị, phải có giao diện thông báo cho người sử dụng về địa điểm (quốc gia) lưu trữ và xử lý dữ liệu

được thu thập bởi thiết bị camera và các dịch vụ liên kết.

8.4. Xóa dữ liệu trên thiết bị camera

a) Có chức năng cho phép người sử dụng xóa dữ liệu được thu thập và lưu trữ trên thiết bị camera.

b) Có chức năng thông báo cho người sử dụng xóa dữ liệu thành công/thất bại trên thiết bị khi thực hiện chức năng xóa.

c) Có chức năng xác nhận người dùng đồng ý xóa dữ liệu trước khi thực hiện xóa.

8.5. Xóa dữ liệu trên dịch vụ liên kết

a) Có chức năng cho phép người sử dụng xóa dữ liệu lưu trữ trên các dịch vụ liên kết.

b) Có chức năng thông báo cho người sử dụng xóa dữ liệu thành công/thất bại trên các dịch vụ liên kết khi thực hiện chức năng xóa.

c) Có chức năng cho phép người sử dụng thiết lập thời gian xóa dữ liệu tự động dữ liệu trên dịch vụ liên kết. Thời gian xóa được người sử dụng thiết lập trên camera hoặc theo thời gian mặc định của nhà sản xuất.

d) Có chức năng xác nhận người sử dụng đồng ý xóa dữ liệu trước khi thực hiện xóa.

9. An toàn ứng dụng

Thiết bị camera phải có các tính năng sau:

a) Kiểm tra tính hợp lệ của dữ liệu đầu vào do người sử dụng nhập hoặc qua giao diện lập trình.

b) Ngăn chặn quá trình xử lý dữ liệu đầu vào vi phạm điều kiện lọc đã định nghĩa trước theo nhà sản xuất.

c) Kiểm tra tính hợp lệ của dữ liệu để ngăn chặn các dạng tấn công vào giao diện của thiết bị. Các dạng tấn công bao gồm nhưng không giới hạn những dạng sau: SQL Injection; OS Command Injection; XPath Injection; Remote File Inclusion (RFI); Local File Inclusion (LFI); Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF).

10. Khả năng tự khôi phục lại hệ thống bình thường sau sự cố

Trong trường hợp thiết bị phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), thiết bị đảm bảo hoạt động bình thường trong lần khởi động kế tiếp./.