BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 21 /2024/TT-BTTTT	*Hà Nội, ngày 31 tháng 12 năm 2024*

THÔNG TƯ

Ban hành "Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu cầu an toàn thông tin cơ bản"

Căn cứ Luật Tiêu chuẩn và Quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

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

Căn cứ Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết và hướng dẫn thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật;

Căn cứ Nghị định số 78/2018/NĐ-CP ngày 16 tháng 5 năm 2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều Luật Tiêu chuẩn và Quy chuẩn kỹ thuật;

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26 tháng 7 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;

Theo đề nghị của Vụ trưởng Vụ Khoa học và Công nghệ,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu cầu an toàn thông tin cơ bản.

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu đảm an toàn thông tin cơ bản (QCVN 135:2024/BTTTT).

Điều 2. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 02 năm 2025.

Điều 3. Lộ trình áp dụng

1. Kể từ ngày 01 tháng 01 năm 2026, thiết bị camera giám sát sử dụng giao thức Internet nhập khẩu và sản xuất trong nước phải đáp ứng các quy định tại QCVN 135:2024/BTTTT.

2. Kể từ ngày 15 tháng 02 năm 2025, QCVN 135:2024/BTTTT được áp dụng trong thử nghiệm, chứng nhận hợp quy, công bố hợp quy.

Điều 4. Tổ chức thực hiện

Chánh Văn phòng, Vụ trưởng Vụ Khoa học và Công nghệ, Thủ trưởng các cơ quan, đơn vị thuộc Bộ Thông tin và Truyền thông, Giám đốc Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này./.

Nơi nhận:
- Thủ tướng Chính phủ, các Phó Thủ tướng Chính phủ (để b/c);
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Sở TTTT các tỉnh, thành phố trực thuộc Trung ương;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng thông tin điện tử của Bộ;
- Lưu: VT, KHCN (250).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 135:2024/BTTTT

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ THIẾT BỊ CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET – CÁC YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN

National technical regulation for Surveillance Camera using Internet Protocol – baseline cybersecurity requirements

HÀ NỘI - 2024

Lời nói đầu

QCVN 135:2024/BTTTT do Cục An toàn thông tin biên soạn, Vụ Khoa học và Công nghệ trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Thông tin và Truyền thông ban hành kèm theo Thông tư số 21 /2024/TT-BTTTT ngày 31 tháng 12 năm 2024.

Mục lục

QUY CHUẨN KỸ THUẬT QUỐC GIA
VỀ THIẾT BỊ CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET – CÁC YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN

National technical regulation
for Surveillance Camera using Internet Protocol – baseline cybersecurity requirements

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn này quy định các yêu cầu kỹ thuật an toàn thông tin mạng cơ bản cho thiết bị camera giám sát sử dụng giao thức Internet.

Thiết bị camera giám sát sử dụng giao thức Internet là camera kỹ thuật số, có thể kết nối qua giao thức Internet, thực hiện một phần hoặc toàn bộ việc giám sát, ghi hình.

Mã số HS của thiết bị camera giám sát sử dụng giao thức Internet áp dụng theo Phụ lục C.

1.2. Đối tượng áp dụng

Quy chuẩn này được áp dụng cho các tổ chức, cá nhân Việt Nam và nước ngoài trên toàn lãnh thổ Việt Nam có hoạt động sản xuất, kinh doanh (bao gồm hoạt động nhập khẩu), khai thác các thiết bị thuộc phạm vi điều chỉnh của quy chuẩn này.

1.3. Tài liệu viện dẫn

ETSI EN 303 645 v2.1.1 (2020-06) "Cyber; Cybersecurity for Consumer Internet of Things: Baseline Requirements".

ETSI TS 103 701 v1.1.1 (2021-08) "Cyber; Cybersecurity for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

1.4. Chữ viết tắt

AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
API	Application Programming Interface	Giao diện lập trình ứng dụng
IP	Internet Protocol	Giao thức Internet
ISO	International Organization for Standardization	Tổ chức Tiêu chuẩn hóa Quốc tế
IXIT	Implementation eXtra Information for Testing	Thông tin triển khai bổ sung cho kiểm thử
ICS	Implementation Conformance Statement	Tuyên bố phù hợp triển khai
MAC	Media Access Control	Điều khiển truy cập môi trường
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ Quốc gia
HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản

HTTPS	HyperText Transfer Protocol Secure	Giao thức truyền tải siêu văn bản an toàn
QR	Quick Response	Phản hồi nhanh
RFC	Request for Comments	Yêu cầu bình luận
SDO	Standards Development Organization	Tổ chức phát triển tiêu chuẩn
SSID	Service Set IDentifier	Nhận diện bộ dịch vụ
SOAP	Simple Object Access Protocol	Giao thức truy cập đối tượng đơn giản
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege	Giả mạo, Làm giả, Phủ nhận, Tiết lộ thông tin, Từ chối dịch vụ, Nâng cao đặc quyền
SWD	Serial Wire Debug	Gỡ lỗi dây nối tiếp
TS	Technical Specification	Thông số kỹ thuật
TLS	Transport Layer Security	An toàn lớp giao vận
UI	User Interface	Giao diện người sử dụng
URL	Uniform Resource Locator	Bộ định vị tài nguyên thống nhất
UART	Universal Asynchronous Receiver-Transmitter	Bộ thu phát không đồng bộ toàn cầu

1.5. Giải thích từ ngữ

Đối với mục đích của quy chuẩn này, các thuật ngữ sau được áp dụng:

1.5.1. Dịch vụ liên kết (Associated services)

Các dịch vụ kỹ thuật số đi kèm với thiết bị camera để cung cấp bổ sung một số chức năng mở rộng của thiết bị.

Ví dụ 1: Các dịch vụ liên quan bao gồm ứng dụng di động, lưu trữ/điện toán đám mây và Giao diện lập trình ứng dụng (API) của bên thứ ba.

Ví dụ 2: Một thiết bị truyền dữ liệu đo đến một dịch vụ của bên thứ ba do nhà sản xuất thiết bị lựa chọn. Dịch vụ này là một dịch vụ liên kết.

1.5.2. Cơ chế xác thực (Authentication mechanism)

Phương pháp được sử dụng để chứng minh tính xác thực của một thực thể.

CHÚ THÍCH: Một "thực thể" là một người sử dụng hoặc máy.

Ví dụ: Một cơ chế xác thực là yêu cầu mật khẩu, quét mã QR hoặc sử dụng máy quét vân tay sinh trắc học.

1.5.3. Giá trị xác thực (Authentication value)

Giá trị cá nhân của một thuộc tính được sử dụng bởi cơ chế xác thực.

Ví dụ: Khi cơ chế xác thực yêu cầu một mật khẩu, giá trị xác thực là một chuỗi ký tự. Khi cơ chế xác thực là định danh vân tay sinh trắc học, giá trị xác thực là vân tay ngón trỏ của tay trái.

1.5.4. Mật mã an toàn (Best practice cryptography)

Mật mã phù hợp với trường hợp sử dụng tương ứng và không có dấu hiệu của một cuộc tấn công khả thi với các kỹ thuật hiện có sẵn.

CHÚ THÍCH 1: Điều này không chỉ đề cập đến các phép mã hóa được sử dụng, mà còn cả việc thực hiện, tạo khóa và xử lý khóa.

CHÚ THÍCH 2: Nhiều tổ chức, chẳng hạn như SDO và cơ quan có thẩm quyền, duy trì hướng dẫn và danh mục các phương pháp mã hóa được sử dụng.

Ví dụ: Nhà sản xuất thiết bị sử dụng một giao thức truyền thông và thư viện mật mã được cung cấp với một nền tảng, thư viện cùng giao thức đó đã được đánh giá khả thi chống lại các cuộc tấn công, chẳng hạn như tấn công phát lại.

1.5.5. Khoảng thời gian hỗ trợ xác định (Defined support period)

Thời gian tối thiểu, được biểu diễn dưới dạng khoảng thời gian hoặc bằng ngày kết thúc, mà nhà sản xuất phải cung cấp các bản cập nhật an toàn.

1.5.6. Nhà sản xuất thiết bị (Device manufacturer)

Đơn vị tạo ra thiết bị camera thành phẩm được lắp ráp, chứa các sản phẩm và thành phần của nhiều nhà cung cấp khác.

1.5.7. Trạng thái mặc định xuất xưởng (Factory default)

Trạng thái của thiết bị sau khi khôi phục cài đặt gốc hoặc sau khi sản xuất/lắp ráp cuối cùng.

CHÚ THÍCH: Điều này bao gồm thiết bị vật lý và phần mềm (bao gồm cả phần mềm hệ thống) có trên thiết bị sau khi lắp ráp.

1.5.8. Nhà sản xuất (Manufacturer)

Các bên liên quan tham gia vào chuỗi cung ứng thiết bị camera (bao gồm nhà sản xuất thiết bị).

CHÚ THÍCH: Ngoài nhà sản xuất thiết bị, các đơn vị như nhà nhập khẩu, nhà phân phối, tích hợp, nhà cung cấp thành phần và nền tảng, nhà cung cấp phần mềm, nhà cung cấp dịch vụ CNTT và viễn thông, nhà cung cấp dịch vụ quản lý và nhà cung cấp dịch vụ liên quan cũng được coi là nhà sản xuất.

1.5.9. 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;...

1.5.10. Cứng hóa (Hard-code)

Nhập dữ liệu trực tiếp vào mã nguồn phần mềm.

1.5.11. Dữ liệu cá nhân (Personal data)

Bất kỳ thông tin nào liên quan đến định danh hoặc có khả năng định danh một con người.

CHÚ THÍCH: Thuật ngữ này được sử dụng để phù hợp với thuật ngữ phổ biến nhưng không có ý nghĩa pháp lý trong quy chuẩn này.

1.5.12. Dữ liệu đo đạc từ xa (Telemetry data)

Dữ liệu từ một thiết bị có khả năng cung cấp thông tin giúp nhà sản xuất xác định các vấn đề hoặc các thông tin liên quan đến việc sử dụng thiết bị.

Ví dụ: Một thiết bị camera báo cáo các lỗi phần mềm cho nhà sản xuất cho phép họ xác định và khắc phục nguyên nhân.

1.5.13. Giá trị duy nhất trên mỗi thiết bị (Unique per device)

Giá trị duy nhất để xác định một thiết bị thuộc cùng một loại sản phẩm nhất định.

1.5.14. 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.

1.5.15. Giao diện gỡ lỗi (Debug interface)

Giao diện vật lý được nhà sản xuất sử dụng để giao tiếp với thiết bị trong quá trình phát triển hoặc để thực hiện phân tích vấn đề của thiết bị và người dùng không được sử dụng giao diện này.

Ví dụ: Điểm thử nghiệm, UART, SWD, JTAG.

1.5.16. Giao diện logic (Logical interface)

Phần mềm sử dụng một giao diện mạng để giao tiếp qua mạng thông qua các kênh hoặc cổng.

1.5.17. Giao diện mạng (Network interface)

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

1.5.18. Giao diện vật lý (Physical interface)

Cổng vật lý hoặc giao diện kết nối vô tuyến được sử dụng để giao tiếp với thiết bị trên lớp vật lý.

Ví dụ: Cổng Ethernet; cổng USB; Wifi.

1.5.19. Mật khẩu khởi tạo (Initial password)

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

1.5.20. Mật khẩu mặc định (Default password)

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

1.5.21. Khởi tạo (Initialization)

Quá trình kích hoạt kết nối mạng của thiết bị để hoạt động và tùy chọn thiết lập các tính năng xác thực cho người sử dụng hoặc cho truy cập mạng.

1.5.22. Tham số an toàn quan trọng (Critical security parameter)

Thông tin bí mật liên quan đến an toàn mà việc tiết lộ hoặc sửa đổi có khả năng làm suy yếu an toàn của một mô-đun an toàn.

Ví dụ: Các khóa mật mã bí mật, giá trị xác thực như mật khẩu, PIN, thành phần riêng của các chứng chỉ.

1.5.23. Tham số an toàn công khai (Public security parameter)

Thông tin công khai liên quan đến an toàn mà việc sửa đổi có khả năng làm suy yếu an toàn của một mô-đun an toàn.

Ví dụ: Thành phần công khai của các chứng chỉ.

1.5.24. Tham số an toàn nhạy cảm (Sensitive security parameter)

Tham số an toàn thuộc một trong hai loại là tham số an toàn quan trọng và tham số an toàn công khai.

1.5.25. Mô-đun an toàn (Security module)

Tập hợp phần cứng, phần mềm và/hoặc phần sụn thực hiện các chức năng an toàn.

Ví dụ: Một thiết bị chứa một root of trust phần cứng, một thư viện mã hóa phần mềm hoạt động trong môi trường thực thi tin cậy, và phần mềm trong hệ điều hành thực thi an toàn như phân tách người sử dụng và cơ chế cập nhật. Tất cả những thứ này tạo thành mô-đun an toàn.

1.5.26. Cập nhật an toàn (Security update)

Cập nhật phần mềm giải quyết các lỗ hổng bảo mật được phát hiện hoặc báo cáo cho nhà sản xuất.

CHÚ THÍCH: Các bản cập nhật phần mềm có thể chỉ là các bản cập nhật an toàn nếu mức độ nghiêm trọng của lỗ hổng yêu cầu một bản sửa lỗi ưu tiên cao hơn.

1.5.27. Dịch vụ phần mềm (software service)

Thành phần phần mềm của một thiết bị được sử dụng để hỗ trợ chức năng.

Ví dụ: Một runtime cho ngôn ngữ lập trình được sử dụng trong phần mềm thiết bị hoặc một daemon cung cấp một API được phần mềm thiết bị sử dụng, ví dụ như API của một mô-đun mật mã.

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

Trạng thái của thiết bị sau khi khởi tạo.

1.5.29. Truy cập từ xa (Remotely accessible)

Truy cập từ bên ngoài mạng nội bộ.

1.5.30. Tuyên bố phù hợp triển khai (Implementation Conformance Statement)

Tuyên bố, được đưa ra bởi nhà cung cấp, về các khả năng được thực hiện hoặc hỗ trợ bởi thiết bị camera.

1.5.31. Tài liệu ICS (Implementation Conformance Statement pro forma)

Tài liệu dưới dạng bảng câu hỏi, được sử dụng để hỗ trợ xây dựng Tuyên bố phù hợp triển khai đối với thiết bị camera.

1.5.32. Thông tin triển khai bổ sung cho kiểm thử (Implementation eXtra Information for Testing)

Hồ sơ chứa hoặc tham chiếu tất cả các thông tin (ngoài thông tin được cung cấp trong ICS) liên quan đến thiết bị camera và môi trường đánh giá của nó, giúp phòng đo kiểm thực hiện các hoạt động kiểm thử tuân thủ.

1.5.33. Tài liệu IXIT (Implementation eXtra Information for Testing pro forma)

Tài liệu dưới dạng bảng câu hỏi, được sử dụng để hỗ trợ xây dựng Thông tin triển khai bổ sung cho kiểm thử đối với thiết bị camera.

1.5.34. Chỉ báo (Indication)

Kết quả được phòng đo kiểm ghi trong tài liệu được sử dụng trong quá trình đánh giá để đưa ra kết luận.

1.5.35. Cam kết an toàn (Security guarantee)

Tuyên bố về các mục tiêu an toàn được giải quyết.

CHÚ THÍCH: Trong tiêu chuẩn này, các Cam kết an toàn được sử dụng trong IXIT để mô tả các mục tiêu an toàn được thực hiện bằng một quy trình hoặc một sự triển khai.

1.5.36. Nhóm kiểm thử (Test group)

Tập hợp các phương pháp kiểm thử liên quan được đặt tên để mô tả cách đánh giá sự tuân thủ của thiết bị camera đối với một quy định trong quy chuẩn này.

CHÚ THÍCH: Tên của các nhóm kiểm thử và các quy định tương ứng của chúng trùng khớp với nhau.

1.5.37. Mục tiêu nhóm kiểm thử (Test group objective)

Mô tả bằng văn bản về mục tiêu kiểm thử trong một nhóm kiểm thử cụ thể được thiết kế.

1.5.38. Mục đích kiểm thử (Test purpose)

Mô tả bằng văn bản về mục đích đánh giá được định nghĩa rõ ràng, tập trung vào một yêu cầu tuân thủ cụ thể hoặc một tập hợp các yêu cầu tuân thủ liên quan.

1.5.39. Kịch bản kiểm thử (Test Scenario)

Tập hợp các nhóm kiểm thử liên quan được đặt tên, mô tả cách đánh giá sự tuân thủ của thiết bị camera đối với một tập hợp các quy định tương ứng trong quy chuẩn này.

CHÚ THÍCH: Tên của các Kịch bản kiểm thử (tập hợp các nhóm kiểm thử) và các tập hợp quy định tương ứng của chúng trùng khớp với nhau.

1.5.40. Bằng chứng bên ngoài (External evidences)

Các chứng nhận an toàn hiện có hoặc các đánh giá của bên thứ ba về các phần của thiết bị camera có thể được sử dụng một phần như là bằng chứng cho sự tuân thủ nhằm giảm thiểu công sức đánh giá.

1.5.41. Đánh giá sự tuân thủ về thiết kế (Test cases conceptual)

Đánh giá sự tuân thủ của IXIT so với các yêu cầu của quy định (sự tuân thủ về thiết kế).

1.5.42. Đánh giá sự tuân thủ về triển khai (Test cases functional)

Đánh giá sự tuân thủ của chức năng của thiết bị camera, mối quan hệ của chúng với các dịch vụ liên kết hoặc quy trình phát triển/quản lý theo yêu cầu của quy định (sự tuân thủ về triển khai).

2. QUY ĐỊNH KỸ THUẬT

2.1. Khởi tạo mật khẩu duy nhất

2.1.1. Yêu cầu 2.1.1

Mật khẩu của thiết bị camera được sử dụng trong bất kỳ trạng thái nào (trừ trạng thái mặc định xuất xưởng) phải là duy nhất cho mỗi thiết bị hoặc do người sử dụng thiết lập.

2.1.2. Yêu cầu 2.1.2

Mật khẩu của thiết bị camera được thiết lập sẵn bởi nhà sản xuất, phải được tạo ra bởi cơ chế có khả năng phòng, chống các cuộc tấn công tự động.

2.1.3. Yêu cầu 2.1.3

Cơ chế xác thực được sử dụng bởi thiết bị camera để xác thực người sử dụng phải sử dụng các mật mã an toàn, phù hợp với mục đích sử dụng, đặc tính công nghệ và nguy cơ, rủi ro.

2.1.4. Yêu cầu 2.1.4

Thiết bị camera có cơ chế cho phép người sử dụng hoặc quản trị viên thay đổi giá trị xác thực một cách đơn giản.

2.1.5. Yêu cầu 2.1.5

Cơ chế xác thực được sử dụng bởi thiết bị camera có khả năng ngăn chặn tấn công vét cạn (brute-force) qua các giao diện mạng.

2.2. Quản lý lỗ hổng bảo mật

2.2.1. Yêu cầu 2.2.1

Nhà sản xuất phải công bố chính sách công bố lỗ hổng bảo mật. Chính sách này phải bao gồm tối thiểu các thông tin sau:

a) Thông tin liên hệ để tiếp nhận thông tin về lỗ hổng;

b) Thông tin về thời gian đối với các việc:

- Xác nhận ban đầu về việc nhận được báo cáo;

- Cập nhật trạng thái xử lý lỗ hổng bảo mật cho đến khi xử lý được các lỗ hổng bảo mật theo báo cáo.

2.3. Quản lý cập nhật

2.3.1. Yêu cầu 2.3.1

Thiết bị camera có cơ chế cập nhật cho phép các phần mềm được cập nhật và cài đặt một cách an toàn.

Ví dụ: Thiết bị camera có các biện pháp phòng, chống để ngăn chặn kẻ tấn công lạm dụng cơ chế cập nhật.

2.3.2. Yêu cầu 2.3.2

Thiết bị camera phải có cơ chế cho phép người sử dụng cập nhật phần mềm một cách đơn giản.

2.3.3. Yêu cầu 2.3.3

Thiết bị camera phải sử dụng các mật mã an toàn để thực hiện đảm bảo an toàn cập nhật.

Ví dụ: Thiết bị camera có cơ chế tự động cập nhật hoặc hỗ trợ người sử dụng cập nhật qua trang thông tin điện tử hoặc ứng dụng di động.

2.3.4. Yêu cầu 2.3.4

Bản cập nhật an toàn phải được nhà sản xuất cung cấp kịp thời.

Ví dụ: Nhà sản xuất phải có chính sách, quy trình về phương án khắc phục lỗ hổng bảo mật được báo cáo, trong đó có đối tượng tham gia và thời gian thực hiện của từng bước.

2.3.5. Yêu cầu 2.3.5

Thiết bị camera có cơ chế kiểm tra tính xác thực và tính toàn vẹn của từng bản cập nhật sử dụng kết nối tin cậy thông qua giao diện mạng.

2.3.6. Yêu cầu 2.3.6

Nhà sản xuất phải công bố thời hạn hỗ trợ bảo hành đối với từng chủng loại thiết bị camera cho người sử dụng.

2.3.7. Yêu cầu 2.3.7

Thiết bị camera cho phép người sử dụng tra cứu thông tin về mã, chủng loại sản phẩm thiết bị thông qua nhãn dán trên thiết bị hoặc qua giao diện vật lý.

2.4. Lưu trữ các tham số an toàn nhạy cảm

2.4.1. Yêu cầu 2.4.1

Các tham số an toàn nhạy cảm phải được lưu trữ an toàn trên bộ nhớ của thiết bị camera.

2.4.2. Yêu cầu 2.4.2

Khi một định danh duy nhất được mã hóa cứng trên camera dùng trong mục đích an toàn, nó phải được bảo vệ để chống lại sự thay đổi bởi các yếu tố vật lý, điện tử hoặc phần mềm.

2.4.3. Yêu cầu 2.4.3

Các tham số an toàn quan trọng mã hóa cứng trong mã nguồn của camera không được sử dụng.

2.4.4. Yêu cầu 2.4.4

Các tham số an toàn quan trọng được sử dụng để kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm và để bảo vệ kết nối giao tiếp với các dịch vụ liên kết, phải là duy nhất cho mỗi thiết bị và phải được tạo ra với một cơ chế có khả năng phòng, chống các cuộc tấn công tự động.

2.5. Quản lý kênh giao tiếp an toàn

2.5.1. Yêu cầu 2.5.1

Thiết bị camera sử phải sử dụng các mật mã an toàn để thiết lập kênh giao tiếp an toàn.

2.5.2. Yêu cầu 2.5.2

Thiết bị camera có chức năng xác thực các đối tượng thực hiện thay đổi liên quan đến an toàn trước khi áp dụng các thay đổi đó. Yêu cầu này không áp dụng đối với các giao thức như: ARP; DHCP; DNS; ICMP; NTP.

Ví dụ: Những thay đổi liên quan đến an toàn bao gồm quản lý quyền, cấu hình khóa mạng và thay đổi mật khẩu.

2.5.3. Yêu cầu 2.5.3

Thiết bị camera phải đảm bảo tính bảo mật của các tham số an toàn quan trọng khi truyền qua môi trường mạng.

2.5.4. Yêu cầu 2.5.4

Nhà sản xuất phải tuân thủ các quy trình quản lý các tham số an toàn quan trọng liên quan đến thiết bị camera.

2.6. Phòng chống tấn công thông qua các giao diện của thiết bị

2.6.1. Yêu cầu 2.6.1

Tất cả giao diện mạng và logic của thiết bị camera mà không được sử dụng phải được vô hiệu hóa.

2.6.2. Yêu cầu 2.6.2

Khi ở trạng thái hoạt động ban đầu, giao diện mạng của thiết bị camera phải giảm thiểu việc tiết lộ các thông tin liên quan đến an toàn khi quá trình xác thực chưa cho kết quả thành công.

2.6.3. Yêu cầu 2.6.3

Trường hợp Camera có giao diện gỡ lỗi có thể truy cập được ở mức vật lý, phải có chức năng vô hiệu hóa giao diện gỡ lỗi bằng phần mềm.

2.7. Bảo vệ dữ liệu người sử dụng

2.7.1. Yêu cầu 2.7.1

Dữ liệu cá nhân nhạy cảm được trao đổi giữa thiết bị camera và các dịch vụ liên kết phải được bảo vệ bằng cách ứng dụng các mật mã phù hợp với mục đích sử dụng và đặc tính công nghệ.

2.7.2. Yêu cầu 2.7.2

Tất cả các chức năng cảm biến bên ngoài của thiết bị camera phải được mô tả đầy đủ và rõ ràng cho người sử dụng.

2.8. Khả năng tự khôi phục lại hoạt động bình thường sau sự cố

2.8.1. Yêu cầu 2.8.1

Thiết bị camera phải có cơ chế khôi phục khi bị mất kết nối mạng hoặc bị mất điện.

2.8.2. Yêu cầu 2.8.2

Thiết bị camera phải hoạt động được bình thường đối với các chức năng nội bộ khi bị mất kết nối mạng và khôi phục được hoàn toàn trạng thái hoạt động sau khi có điện trở lại.

2.8.3. Yêu cầu 2.8.3

Thiết bị camera khôi phục lại kết nối mạng theo một cách trình tự và ổn định.

2.9. Xóa dữ liệu trên thiết bị camera

2.8.1. Yêu cầu 2.9.1

Thiết bị camera có chức năng cho phép xóa dữ liệu người sử dụng trên thiết bị camera.

2.10. Xác thực dữ liệu đầu vào

2.10.1. Yêu cầu 2.10.1

Phần mềm của thiết bị camera phải xác thực dữ liệu đầu vào từ các giao diện người sử dụng hoặc được truyền qua các giao diện lập trình ứng dụng (API) hoặc giữa các dịch vụ và thiết bị.

2.11. Bảo vệ dữ liệu trên thiết bị camera

2.11.1. Yêu cầu 2.11.1

Nhà sản xuất phải cung cấp đầy đủ thông tin về mục đích, cách thức thu thập, xử lý và lưu trữ dữ liệu cá nhân được thu thập và xử lý bởi thiết bị camera, dịch vụ liên kết hoặc bên thứ ba (nếu có).

2.11.2. Yêu cầu 2.11.2

Thiết bị camera phải có chức năng xác nhận sự đồng ý của người sử dụng đối với việc cho phép thiết bị camera thu thập và xử lý dữ liệu cá nhân.

2.11.3. Yêu cầu 2.11.3

Thiết bị camera phải có chức năng cho phép người sử dụng thu hồi sự đồng ý đối với việc cho phép thiết bị camera thu thập và xử lý dữ liệu cá nhân.

2.11.4. Yêu cầu 2.11.4

Dữ liệu đo đạc từ xa được thu thập từ thiết bị camera phải được mô tả đầy đủ về mục đích, đối tượng thu thập và nơi lưu trữ.

2.11.5. Yêu cầu 2.11.5

Thiết bị camera có chức năng cho phép thiết lập cấu hình để lưu trữ dữ liệu tại Việt Nam.

3. PHƯƠNG PHÁP ĐO

3.1. Khởi tạo mật khẩu duy nhất

3.1.1. Nhóm kiểm thử yêu cầu 2.1.1

3.1.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.1.1, điều 2.1.1 Quy chuẩn này.

Nhóm kiểm thử này áp dụng với tất cả các trạng thái của thiết bị camera ngoại trừ trạng thái mặc định xuất xưởng.

3.1.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế xác thực dựa trên mật khẩu.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá tất cả các cơ chế xác thực dựa trên mật khẩu trong **IXIT 1-AuthMech** với các mật khẩu không được người sử dụng định nghĩa theo "Yếu tố xác thực" và được sử dụng trong bất kỳ trạng thái nào của thiết bị camera ngoại trừ trạng thái mặc định xuất xưởng, trong khi đó thông tin về "Cơ chế khởi tạo mật khẩu" được sử dụng để đảm bảo rằng các mật khẩu là duy nhất trên mỗi thiết bị.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mỗi mật khẩu được tạo ra trong mỗi cơ chế xác thực dựa trên mật khẩu của thiết bị camera, được sử dụng trong bất kỳ trạng thái nào ngoại trừ trạng thái mặc định xuất xưởng và không được định nghĩa bởi người sử dụng, là duy nhất trên mỗi thiết bị.

c2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.1.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế xác thực dựa trên mật khẩu bao gồm tính đầy đủ của tài liệu **IXIT (b1)**, các mật khẩu do người sử dụng định nghĩa (b2) và các cơ chế khởi tạo mật khẩu (b3).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá các cơ chế khởi tạo mật khẩu không được tài liệu hóa trong **IXIT 1-AuthMech** có tồn tại thông qua giao diện mạng trên thiết bị camera hoặc được mô tả trong hướng dẫn sử dụng.

b2) Đối với mỗi cơ chế xác thực dựa trên mật khẩu của người sử dụng trong **IXIT 1-AuthMech**, Phòng đo kiểm đánh giá liệu người sử dụng có bắt buộc phải định nghĩa tất cả các mật khẩu mà được yêu cầu phải định nghĩa bởi người sử dụng theo "Yếu tố xác thực" trước khi được sử dụng hay không.

b3) Phòng đo kiểm đánh giá liệu tất cả các mật khẩu của thiết bị camera mà không được người sử dụng định nghĩa theo "Yếu tố xác thực" trong **IXIT 1-AuthMech** và được sử dụng ở bất kỳ trạng thái nào khác ngoài trạng thái mặc định xuất xưởng, không được vi phạm phần mô tả về "Cơ chế khởi tạo mật khẩu".

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mỗi cơ chế xác thực dựa trên mật khẩu được mô tả đầy đủ trong **IXIT**.

• Người sử dụng được yêu cầu định nghĩa tất cả các mật khẩu trước khi sử dụng đối với những loại mật khẩu được yêu cầu định nghĩa bởi người sử dụng trong **IXIT**.

• Không có dấu hiệu cho thấy việc khởi tạo mật khẩu mà không được người sử dụng định nghĩa trên thiết bị camera trong bất kỳ trạng thái nào khác ngoài trạng thái mặc định xuất xưởng khác biệt với cơ chế khởi tạo mật khẩu như mô tả trong **IXIT**.

c2) Không đáp ứng: Nếu một trong các yêu cầu trên không đáp ứng.

3.1.2. Nhóm kiểm thử yêu cầu 2.1.2

3.1.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.1.2, điều 2.1.2 Quy chuẩn này.

3.1.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế khởi tạo đối với mật khẩu được cài đặt sẵn.

b) Phương pháp kiểm thử

b1) Đánh giá mỗi cơ chế xác thực trong IXIT 1-AuthMech sử dụng các mật khẩu được cài đặt sẵn theo "Yếu tố xác thực", liệu cơ chế khởi tạo trong "Cơ chế khởi tạo mật khẩu" có mô tả các quy tắc rõ ràng cho khởi tạo mật khẩu hay không.

CHÚ THÍCH 1: Các bộ đếm tăng dần (chẳng hạn như "password1", "password2",...) là các quy tắc rõ ràng.

b2) Đánh giá liệu cơ chế khởi tạo mật khẩu có tạo ra các chuỗi mật khẩu hoặc các quy luật thông dụng trong các mật khẩu hay không.

CHÚ THÍCH 2: Chuỗi mật khẩu thông dụng được định nghĩa trong các từ điển mật khẩu phổ biến, công khai trên https://www.ais.gov.vn.

b3) Đánh giá liệu cơ chế khởi tạo mật khẩu có tạo ra các mật khẩu chứa các thông tin công khai hay không.

CHÚ THÍCH 3: Thông tin công khai bao gồm địa chỉ MAC, SSID Wi-Fi®, tên, loại và mô tả của thiết bị.

b4) Đánh giá liệu cơ chế khởi tạo mật khẩu có tạo ra các mật khẩu đáp ứng các yêu cầu về độ phức tạp.

CHÚ THÍCH 4: Độ phức tạp có liên quan tới xác suất đoán được mật khẩu dựa trên thông tin mà kẻ tấn công đã nắm được. Độ dài mật khẩu cũng là một trong những tiêu chí quan trọng đối với độ phức tạp của mật khẩu.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Không có quy tắc rõ ràng trong các mật khẩu được cài đặt sẵn.
- Không tìm thấy các chuỗi thông dụng hoặc có quy luật thông dụng trong các mật khẩu được cài đặt sẵn.
- Các cơ chế khởi tạo mật khẩu không tạo các mật khẩu được cài đặt sẵn có liên quan đến thông tin công khai.
- Các cơ chế khởi tạo mật khẩu tạo các mật khẩu được cài đặt sẵn đáp ứng các yêu cầu về độ phức tạp.

c2) Không đáp ứng: Nếu một trong các yêu cầu trên không đáp ứng.

3.1.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế khởi tạo đối với mật khẩu được cài đặt sẵn.

b) Phương pháp kiểm thử

b1) Đối với mỗi cơ chế xác thực trong IXIT 1-AuthMech sử dụng mật khẩu được cài đặt sẵn theo "Yếu tố xác thực", phòng đo kiểm đánh giá liệu cơ chế khởi tạo mật khẩu có được triển khai tuân thủ theo mô tả trong "Cơ chế khởi tạo mật khẩu" hay không.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá có chức năng đáp ứng các yêu cầu, bao gồm:

- Đối với mỗi mật khẩu được khởi tạo sẵn, không có dấu hiệu cho thấy việc khởi tạo mật khẩu là khác biệt so với cơ chế khởi tạo được mô tả trong IXIT.

c2) Không đáp ứng: Nếu yêu cầu ở trên không đáp ứng.

3.1.3. Nhóm kiểm thử yêu cầu 2.1.3

3.1.3.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.1.3, điều 2.1.3 Quy chuẩn này.

Theo Quy chuẩn này, Mật mã an toàn được định nghĩa là mật mã phù hợp với từng trường hợp sử dụng tương ứng và không khả thi để bị tấn công bằng các kỹ thuật hiện có.

Mục đích của nhóm kiểm thử này là để xác nhận rằng các phương thức mã hóa cung cấp Cam kết an toàn cần thiết cho các cơ chế xác thực và các phương thức mã hóa này được biết là không dễ bị tấn công.

3.1.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các phương pháp mã hoá được sử dụng trong các cơ chế xác thực, bao gồm việc sử dụng Mật mã an toàn (b1, b2, b3) và khả năng bị tấn công (b4).

b) Phương pháp kiểm thử

b1) Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** được sử dụng để xác thực người sử dụng với thiết bị camera, Phòng đo kiểm đánh giá các "Cam kết an toàn" đáp ứng trong trường hợp xác thực người sử dụng, ít nhất đáp ứng các yêu cầu về tính toàn vẹn và xác thực.

b2) Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** được sử dụng để xác thực người dùng với thiết bị camera, Phòng đo kiểm đánh giá cơ chế xác thực được mô tả trong "Mô tả" có đảm bảo được các "Cam kết an toàn" hay không.

CHÚ THÍCH: Cần có phương pháp tiếp cận tổng thể để đánh giá về tính an toàn của cơ chế.

b3) Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** được sử dụng để xác thực người sử dụng với thiết bị camera, Phòng đo kiểm đánh giá "Phương thức mã hóa" có sử dụng Mật mã an toàn tuân thủ các quy định, tiêu chuẩn kỹ thuật của cơ quan quản lý liên quan hoặc tiêu chuẩn quốc tế tương đương. Nếu "Phương thức mã hóa" không có trong danh mục tham khảo cho trường hợp sử dụng tương ứng, nhà cung cấp phải cung cấp bằng chứng, ví dụ như phân tích rủi ro, để chứng minh rằng mật mã đó là phù hợp cho trường hợp sử dụng. Trong trường hợp đó, Phòng đo kiểm phải đánh giá liệu bằng chứng có phù hợp và đáng tin cậy cho trường hợp sử dụng hay không.

CHÚ THÍCH: Một thuật toán mật mã hoặc một mật mã nguyên thủy lỗi thời liên quan đến thuộc tính an toàn của nó (ví dụ như SHA-1 vì dễ trùng lặp) hoặc dựa trên một tham số mật mã (ví dụ như kích thước khóa) là không phù hợp, khi xét tới thời gian sử dụng dự kiến của thiết bị camera và tính linh hoạt của mật mã thì không được coi là Mật mã an toàn.

b4) Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** được sử dụng để xác thực người sử dụng, Phòng đo kiểm đánh giá "Phương thức mã hóa" không dễ bị tấn công với các thuộc tính an toàn được thiết lập dựa trên "Cam kết an toàn" bằng cách tham chiếu đến các báo cáo phân tích mật mã đủ điều kiện.

CHÚ THÍCH: Các báo cáo phân tích mật mã đủ điều kiện bao gồm các bài nghiên cứu được xuất bản trên các tạp chí khoa học, hoặc được cung cấp bởi chính nhà sản xuất. Ngoài ra, tham chiếu tới **Phụ lục B.2** về những rủi ro an toàn cơ bản có khả năng xảy ra.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu đối với toàn bộ các cơ chế xác thực người sử dụng, bao gồm:

• Các "Cam kết an toàn" đáp ứng trong trường hợp xác thực người sử dụng;

• Cơ chế đáp ứng được các "Cam kết an toàn" liên quan đến trường hợp sử dụng;

• Tất cả các "Phương thức mã hóa" được sử dụng là mật mã an toàn đối với trường hợp sử dụng;

• Tất cả các "Phương thức mã hóa" không được biết là dễ bị tấn công với các thuộc tính an toàn.

c2) Không đáp ứng: Nếu một trong các yêu cầu trên không đáp ứng.

3.1.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các mật mã được sử dụng trong các cơ chế xác thực.

b) Phương pháp kiểm thử

Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech**, Phòng đo kiểm đánh giá thiết bị camera có sử dụng các "Phương thức mã hoá" được mô tả hay không.

Ví dụ: Trong trường hợp xác thực dựa trên chứng chỉ PKI, việc sử dụng công cụ sniffer để thu thập chứng chỉ và so sánh các thuộc tính với phương pháp mã hoá được mô tả trong **IXIT** hữu ích để thu thập chỉ báo.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Bất kỳ phương thức mã hoá được sử dụng phải tuân thủ theo mô tả trong **IXIT**.

c2) Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

3.1.4. Nhóm kiểm thử yêu cầu 2.1.4

3.1.4.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.1.4, điều 2.1.4 Quy chuẩn này.

3.1.4.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế thay đổi giá trị xác thực.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** mà thông tin trong phần "Mô tả" cho thấy cơ chế được sử dụng để xác thực người sử dụng, thông tin về "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo** có xem xét đến cơ chế này và mô tả dễ hiểu cách thức thay đổi giá trị xác thực cho người sử dụng có kiến thức kỹ thuật hạn chế (tham khảo **Phụ lục B.3**).

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với tất cả các cơ chế xác thực người sử dụng, các tài nguyên đã xuất bản mô tả cách thức thay đổi giá trị xác thực một cách đơn giản.

c2) Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

3.1.4.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế thay đổi giá trị xác thực.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm thực hiện thay đổi các giá trị xác thực cho tất cả các cơ chế xác thực người sử dụng trong **IXIT 1-AuthMech** theo hướng dẫn được mô tả theo "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo.**

b2) Phòng đo kiểm đánh giá các giá trị xác thực được thay đổi thành công.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Tất cả các cơ chế cho phép người sử dụng thay đổi giá trị xác thực hoạt động đúng như mô tả.

c2) Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

3.1.5. Nhóm kiểm thử yêu cầu 2.1.5

3.1.5.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.1.5, điều 2.1.5 Quy chuẩn này.

3.1.5.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc cơ chế khiến việc tấn công vét cạn thông qua giao diện mạng trở nên bất khả thi.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech** với phần "Mô tả" cho thấy cơ chế có thể truy cập trực tiếp qua giao diện mạng, cơ chế trong "Ngăn chặn tấn công vét cạn" có khiến việc tấn công vét cạn thông qua giao diện mạng trở nên bất khả thi.

CHÚ THÍCH: Các phương pháp giảm thiểu tấn công vét cạn bao gồm, nhưng không giới hạn:

• Thời gian trì hoãn giữa các lần thử xác thực liên tiếp bị thất bại.

• Giới hạn số lần thử xác thực, sau đó là một khoảng thời gian tạm dừng cho phép đăng nhập.

• Giới hạn số lần thử xác thực, sau đó khóa cơ chế xác thực.

• Đảm bảo độ entropy phù hợp cho các giá trị xác thực dựa trên mật mã an toàn.

• Xác thực hai yếu tố.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Cơ chế được tài liệu hoá khiến việc tấn công vét cạn thông qua giao diện mạng trở nên bất khả thi.

c2) Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

3.1.5.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc cơ chế khiến việc tấn công vét cạn thông qua giao diện mạng trở nên bất khả thi, bao gồm tính đầy đủ của tài liệu **IXIT** (b1) và các cơ chế tương ứng (b2).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu có tồn tại các cơ chế xác thực qua giao diện mạng khác mà không được mô tả trong **IXIT 1-AuthMech**.

CHÚ THÍCH: Các phương thức để kiểm tra các cơ chế xác thực qua giao diện mạng bao gồm các công cụ rà quét mạng như "nmap" hoặc công cụ sniffer không dây như thiết bị dongle BLE.

b2) Phòng đo kiểm thử nghiệm tấn công vét cạn đối với mỗi cơ chế xác thực qua giao diện mạng được mô tả trong **IXIT 1-AuthMech**.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Tất cả các cơ chế xác thực qua giao diện mạng của sản phẩm được mô tả trong **IXIT 1-AuthMech**.

• Đối với mỗi cơ chế xác thực qua giao diện mạng, việc triển khai phương án ngăn chặn tấn công vét cạn tuân thủ theo tài liệu **IXIT** tương ứng.

c2) Không đáp ứng: Nếu một trong các yêu cầu trên không đáp ứng.

3.2. Quản lý lỗ hổng bảo mật

3.2.1. Nhóm kiểm thử yêu cầu 2.2.1

3.2.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế và có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.2.1, điều 2.2.1 Quy chuẩn này.

3.2.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với chính sách công bố thông tin về lỗ hổng bảo mật.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc truy cập vào công bố như mô tả trong "Chính sách tiết lộ lỗ hổng" trong **IXIT 2-UserInfo** có thể thực hiện được mà không cần đáp ứng các tiêu chí như tài khoản người sử dụng, là liệu bất kỳ ai cũng truy cập vào tài liệu hay không.

CHÚ THÍCH: Một trang trang thông tin điện tử của nhà sản xuất được coi là đáp ứng.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Chính sách công bố lỗ hổng bảo mật được công khai với bất kỳ ai.

c2) Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

3.2.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với chính sách công bố thông tin về lỗ hổng bảo mật.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu chính sách công bố lỗ hổng bảo mật có thể truy cập công khai như được mô tả trong phần "Chính sách tiết lộ lỗ hổng" trong **IXIT 2-UserInfo** hay không.

b2) Phòng đo kiểm đánh giá chính sách có cung cấp thông tin bao gồm:

- Thông tin liên hệ;
- Thông tin về thời gian liên quan đến việc tiếp nhận thông tin và cập nhật trạng thái.

CHÚ THÍCH: Thông tin về thời gian cung cấp sự linh hoạt để mô tả các giá trị thời gian (ví dụ: "7 ngày", "lập tức"). Hơn nữa, nó cũng cho phép mô tả làm thế nào để tạo ra một dòng thời gian trong trường hợp có một lỗ hổng được báo cáo.

c) Kết luận

c1) Đáp ứng: Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Chính sách công bố lỗ hổng bảo mật được công khai;
- Chính sách công bố lỗ hổng bảo mật bao gồm các thông tin liên hệ và dòng thời gian về thời gian tiếp nhận thông tin và cập nhật trạng thái.

c2) Không đáp ứng: Nếu một trong các yêu cầu trên không đáp ứng.

3.3. Quản lý cập nhật

3.3.1. Nhóm kiểm thử yêu cầu 2.3.1

3.3.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.1, điều 2.3.1 Quy chuẩn này.

Nhóm kiểm thử này kiểm tra tồn tại ít nhất một cơ chế cập nhật cho việc cài đặt an toàn các bản cập nhật phần mềm.

3.3.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với cơ chế cập nhật của các thành phần phần mềm tồn tại đầy đủ biện pháp ngăn chặn không cho phép kẻ tấn công lợi dụng cơ chế cập nhật trên thiết bị camera.

b) Phương pháp kiểm thử

Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, đánh giá cơ chế cập nhật có khả năng ngăn chặn được các hình thức tấn công mạng dựa vào các mô tả tại "Cam kết an toàn", "Mô tả", "Phương thức mã hóa" và "Khởi tạo và tương tác" hay không.

CHÚ THÍCH: Xem xét mô hình tấn công cơ bản được mô tả trong **Phụ lục B.2** là hữu ích cho việc kiểm tra.

Ví dụ: Việc lợi dụng để tấn công bao gồm việc cài đặt một bản cập nhật phần mềm cũ để hạ cấp các biện pháp an toàn của thiết bị camera hoặc chèn mã độc bằng cách thao túng một bản cập nhật hợp lệ.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Cơ chế cập nhật của thiết bị camera không bị lợi dụng bởi kẻ tấn công.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.3.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với khả năng ngăn chặn việc lợi dụng của cơ chế cập nhật.

b) Phương pháp kiểm thử

b1) Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm thực hiện các kịch bản tấn công để lợi dụng cơ chế cập nhật dựa trên phần "Mô tả".

CHÚ THÍCH 1: Một cuộc tấn công bao gồm việc cố gắng tiếp tục một chuỗi các bước cập nhật sau khi một bước cập nhật cụ thể thất bại, cài đặt một phiên bản phần mềm cũ hơn có chứa lỗ hổng bảo mật hoặc thay đổi một byte trong phần mềm đã ký (signed) để kiểm tra xem nó có bị từ chối hay không.

CHÚ THÍCH 2: Có nhiều cách để thực hiện một chỉ báo dựa trên phân tích an toàn ngay cả khi không có bản cập nhật nào trong quá trình đánh giá, ví dụ như xác minh cơ chế cập nhật dựa trên tập tin trên cơ sở các gói cập nhật cũ.

b2) Phòng đo kiểm thử nghiệm việc lợi dụng mỗi cơ chế cập nhật dựa trên các hành động bất lợi đã được thiết kế và đánh giá liệu thiết kế của cơ chế (dựa vào thông tin được mô tả tại phần "Mô tả", "Phương thức mã hóa" và "Khởi tạo và tương tác") có khả năng ngăn chặn hiệu quả việc lợi dụng các bản cập nhật phần mềm như mô tả về "Cam kết an toàn".

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Không khả thi trong việc lợi dụng một cơ chế cập nhật trên thiết bị camera.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.3.2. Nhóm kiểm thử yêu cầu 2.3.2

3.3.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera được thiết kế có các chức năng, tính năng kỹ thuật đáp ứng yêu cầu 2.3.2, điều 2.3.2 Quy chuẩn này.

Theo Quy chuẩn, trong nhóm kiểm thử này, một bản cập nhật đơn giản để áp dụng bao gồm việc áp dụng tự động, hoặc được khởi tạo bằng cách sử dụng một dịch vụ liên quan (chẳng hạn như một ứng dụng di động) hoặc qua giao diện trang thông tin điện tử trên thiết bị. Điều này không loại trừ các giải pháp thay thế.

Trọng tâm của quy định là kích hoạt cập nhật từ phía người sử dụng và xác minh liệu người sử dụng có được cung cấp khả năng cập nhật tất cả các thành phần phần mềm một cách đơn giản hay không. Điều này được xác định nếu mỗi thành phần phần mềm được cập nhật với ít nhất một cơ chế cập nhật đơn giản.

3.3.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế cập nhật đơn giản cho người sử dụng thực hiện cập nhật phần mềm.

b) Phương pháp kiểm thử

b1) Đối với mỗi thành phần phần mềm trong **IXIT 6-SoftComp**, Phòng đo kiểm đánh giá có tồn tại ít nhất một "Cơ chế cập nhật" được mô tả, và sự đơn giản để người sử dụng áp dụng theo thông tin về "Khởi tạo và tương tác" trong **IXIT 7-UpdMech** đáp ứng ít nhất một trong các yếu tố sau:

• Bản cập nhật phần mềm được áp dụng tự động mà không yêu cầu bất kỳ sự tương tác nào từ người sử dụng;

• Bản cập nhật phần mềm được khởi tạo thông qua một dịch vụ liên quan;

• Bản cập nhật phần mềm được khởi tạo thông qua giao diện trang thông tin điện tử trên thiết bị;

• Bản cập nhật phần mềm sử dụng phương thức tương tự phù hợp với người sử dụng có kiến thức kỹ thuật hạn chế (tại **Phụ lục B.3**)

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mỗi thành phần phần mềm hỗ trợ ít nhất một cơ chế cập nhật đơn giản để người sử dụng áp dụng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.3.3. Nhóm kiểm thử yêu cầu 2.3.3

3.3.3.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.3, điều 2.3.3 Quy chuẩn này.

Theo Quy chuẩn này, Mật mã an toàn được định nghĩa là phù hợp với từng trường hợp sử dụng tương ứng và không khả thi để bị tấn công bằng các kỹ thuật hiện nay.

Mục đích của nhóm kiểm thử này là để xác nhận rằng các phương pháp mã hóa đảm bảo về tính an toàn cần thiết cho các cơ chế cập nhật an toàn và liệu các phương pháp mã hóa này không được biết tới là rủi ro cho một cuộc tấn công.

3.3.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các phương pháp mã hoá sử dụng trong các cơ chế cập nhật bao gồm việc sử dụng mật mã an toàn (b1, b2, b3) và khả năng bị tấn công (b4).

b) Phương pháp kiểm thử

b1) Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá các "Cam kết an toàn" đáp ứng trong trường hợp cập nhật an toàn, ít nhất đáp ứng các yêu cầu về tính toàn vẹn và xác thực.

b2) Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá liệu cơ chế này theo như thông tin trong phần "Mô tả" có phù hợp để đạt được "Cam kết an toàn" hay không.

CHÚ THÍCH: Cần có phương pháp tiếp cận tổng thể để đánh giá về tính an toàn của cơ chế.

b3) Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá "Phương thức mã hóa" có sử dụng Mật mã an toàn tuân thủ các quy định, tiêu chuẩn kỹ thuật của cơ quan quản lý liên quan hoặc tiêu chuẩn quốc tế tương đương. Nếu "Phương thức mã hóa" không có trong danh mục tham khảo cho trường hợp sử dụng tương ứng, nhà cung cấp phải cung cấp bằng chứng, ví dụ như phân tích rủi ro, để chứng minh rằng mật mã đó là phù hợp cho trường hợp sử dụng. Trong trường hợp đó, Phòng đo kiểm phải đánh giá liệu bằng chứng có phù hợp và đáng tin cậy cho trường hợp sử dụng hay không.

CHÚ THÍCH: Một thuật toán hoặc một phương thức đã lỗi thời do thuộc tính an toàn của nó (ví dụ: SHA-1 vì dễ trùng lặp) hoặc phương pháp mã hóa dựa trên một tham số mật mã (ví dụ: kích thước khóa) không phù hợp, khi xem xét tới thời gian sử dụng dự kiến của thiết bị và khả năng bảo đảm của mật mã thì không được coi là Mật mã an toàn.

b4) Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá "Phương thức mã hóa" không dễ bị tấn công với các thuộc tính được thiết lập dựa trên thông tin về "Cam kết an toàn" bằng cách tham chiếu đến các báo cáo phân tích mật mã có thẩm quyền.

CHÚ THÍCH: Các báo cáo phân tích mật mã có thẩm quyền bao gồm các bài nghiên cứu được xuất bản trên các tạp chí khoa học, hoặc được cung cấp bởi chính nhà sản xuất. Ngoài ra, tham chiếu tới **Phụ lục B.2** về những rủi ro an toàn cơ bản có khả năng xảy ra.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với toàn bộ các cơ chế cập nhật, bao gồm:

- Các Cam kết an toàn đáp ứng trong các trường hợp cập nhật an toàn;
- Cơ chế đáp ứng được các Cam kết an toàn đối với trường hợp sử dụng;
- Tất cả các "Phương thức mã hóa" được sử dụng coi là Mật mã an toàn đối với trường hợp sử dụng;
- Tất cả các "Phương thức mã hóa" không được biết là dễ bị tấn công với các thuộc tính an toàn.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.3.4. Nhóm kiểm thử yêu cầu 2.3.4

3.3.4.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.4, điều 2.3.4 Quy chuẩn này.

Nhóm kiểm thử này tập trung vào các quy trình quản lý cần thiết để triển khai các bản cập nhật an toàn kịp thời.

3.3.4.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với cách thức triển khai các bản cập nhật an toàn (b1) và xác nhận rằng các điều kiện tiên quyết cho việc triển khai đã được đảm bảo (b2).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu thông tin về "Mô tả" và "Khung thời gian" của mỗi quy trình cập nhật an toàn trong **IXIT 8-UpdProc** hỗ trợ việc triển khai các bản cập nhật an toàn một cách kịp thời.

CHÚ THÍCH 1: Xem xét mức độ nghiêm trọng và tầm quan trọng của các lỗ hổng bảo mật được đề cập và loại lỗ hổng (ví dụ: phần mềm nhúng, phần cứng hoặc phần mềm) là hữu ích.

CHÚ THÍCH 2: Mức độ hợp tác giữa các thực thể liên quan, số lượng các bước quy trình và trách nhiệm được xác định rõ ràng là các chỉ báo quan trọng để triển khai kịp thời.

CHÚ THÍCH 3: Trong trường hợp có sự tham gia của bên thứ ba (ví dụ: nhà cung cấp thư viện phần mềm), việc tài liệu hóa các đầu mối liên lạc và quy trình hợp tác được xác định là các chỉ báo cho việc triển khai kịp thời.

CHÚ THÍCH 4: So sánh với khung thời gian cho các bản cập nhật an toàn của các sản phẩm tương tự là hữu ích.

b2) Phòng đo kiểm đánh giá thông tin về "Xác nhận quy trình cập nhật" trong **IXIT 4-Conf** có xác nhận hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Quy trình quản lý cập nhật đáp ứng yêu cầu về cập nhật an toàn kịp thời;
- Có xác nhận về việc triển khai.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu ở trên không đáp ứng.

3.3.5. Nhóm kiểm thử yêu cầu 2.3.5

3.3.5.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.5, điều 2.3.5 Quy chuẩn này.

CHÚ THÍCH: Phần "Mô tả" trong **IXIT 7-UpdMech** cho biết liệu đó có phải là cơ chế cập nhật dựa trên giao diện mạng.

Việc xác thực mối quan hệ tin cậy là cần thiết để đảm bảo rằng một đối tượng không được ủy quyền (ví dụ: nền tảng quản lý thiết bị camera hoặc chính thiết bị camera) không thể cài đặt mã độc.

Trọng tâm của nhóm kiểm thử này là việc xác minh tính xác thực và toàn vẹn phải được thực hiện thông qua một mối quan hệ tin cậy, tức là việc xác minh dựa trên các hành động liên quan đến một đối tượng được ủy quyền (ví dụ: xác nhận bởi người sử dụng được ủy quyền).

3.3.5.2. Đánh giá sự tuân thủ về thiết kế và triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc xác minh các bản cập nhật phần mềm thông qua mối quan hệ tin cậy bao gồm tính xác thực và toàn vẹn (b1) và đối tượng thực hiện (b2), cùng với việc đánh giá sự tuân thủ về triển khai đối với tính đầy đủ của tài liệu **IXIT**.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm áp dụng các phương pháp kiểm thử được chỉ định bao gồm:

- Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá tính xác thực của các bản cập nhật phần mềm đáp ứng theo thông tin về "Cam kết an toàn" và "Phương thức mã hoá" tương ứng, bao gồm, đặc biệt là tính nguyên bản của bản cập nhật phần mềm liên quan đến nguồn gốc (nhà sản xuất) và thiết bị camera trước khi cài đặt.

CHÚ THÍCH 1: Có nhiều cách khác nhau để xác minh tính nguyên bản của một bản cập nhật phần mềm liên quan đến nguồn gốc và thiết bị camera.

CHÚ THÍCH 2: Việc xác minh tính xác thực bởi chính thiết bị camera chủ yếu nhằm từ chối các bản cập nhật phần mềm không được tin cậy.

- Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, Phòng đo kiểm đánh giá tính toàn vẹn của các bản cập nhật phần mềm đáp ứng theo thông tin về "Cam kết an toàn" và "Phương thức mã hoá" tương ứng.

CHÚ THÍCH 3: Việc xác minh tính toàn vẹn bởi chính thiết bị camera chủ yếu nhằm phát hiện mã độc được chèn vào trong một bản cập nhật phần mềm hợp lệ.

b2) Đối với mỗi cơ chế cập nhật dựa trên giao diện mạng trong **IXIT 7-UpdMech**, Phòng đo kiểm xác minh tính toàn vẹn và tính xác thực có dựa trên một mối quan hệ tin cậy hợp lệ theo thông tin trong phần "Mô tả" và "Cam kết an toàn". Một mối quan hệ tin cậy hợp lệ bao gồm một trong những yêu cầu sau:

- Kênh truyền được xác thực;
- Tham gia một mạng lưới yêu cầu thiết bị camera sở hữu một tham số bảo mật quan trọng hoặc mật khẩu để tham gia;
- Xác minh bằng chữ ký số của bản cập nhật;
- Xác nhận bởi người sử dụng;
- Một chức năng bảo mật tương đương.

b3) Phòng đo kiểm đánh giá các cơ chế cập nhật không được tài liệu hóa trong **IXIT 7-UpdMech** có tồn tại thông qua một giao diện mạng trên thiết bị camera hay không.

Ví dụ: Các công cụ rà quét mạng cho phép phát hiện các cơ chế cập nhật dựa trên giao diện mạng.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Mỗi cơ chế cập nhật minh chứng được tính hiệu quả trong việc xác minh tính xác thực của các bản cập nhật phần mềm;
- Mỗi cơ chế cập nhật minh chứng được tính hiệu quả trong việc xác minh tính toàn vẹn của các bản cập nhật phần mềm;
- Xác minh được tính xác thực và toàn vẹn của các bản cập nhật phần mềm là dựa trên một mối quan hệ tin cậy hợp lệ;
- Mọi cơ chế cập nhật dựa trên giao diện mạng được phát hiện đều được mô tả trong **IXIT**.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu ở trên không đáp ứng.

3.3.6. Nhóm kiểm thử yêu cầu 2.3.6

3.3.6.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.6, điều 2.3.6 Quy chuẩn này.

Khoảng thời gian hỗ trợ xác định là mô tả khoảng thời gian mà nhà sản xuất cung cấp hỗ trợ liên quan đến các bản cập nhật phần mềm. Thời gian hỗ trợ cập nhật phần mềm được định nghĩa dự kiến được công bố ngay cả khi không có bản cập nhật phần mềm nào được hỗ trợ, trong trường hợp này nó thể hiện không có các bản cập nhật phần mềm.

3.3.6.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc công bố thời gian hỗ trợ.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc truy cập thông tin về "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có dễ hiểu và dễ nắm bắt đối với người sử dụng có kiến thức kỹ thuật hạn chế (theo quy định tại **Phụ lục B.3**).

Ví dụ: Với sự trợ giúp từ Model thiết bị camera, người sử dụng tìm thấy thời gian hỗ trợ thông qua công cụ tìm kiếm trên trang trang thông tin điện tử của nhà sản xuất.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Việc công bố thời gian hỗ trợ cập nhật phần mềm dễ hiểu đối với người sử dụng có kiến thức kỹ thuật hạn chế.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.3.6.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc công bố thời gian hỗ trợ.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc truy cập thông tin công bố thời gian hỗ trợ theo mô tả trong phần "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có được cung cấp cho người sử dụng như mô tả.

b2) Phòng đo kiểm đánh giá có thể truy cập công khai không giới hạn (ví dụ: yêu cầu đăng ký trước khi truy cập) thông tin công bố thời gian hỗ trợ theo mô tả trong phần "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo**.

b3) Phòng đo kiểm đánh giá thời gian hỗ trợ được công bố theo thông tin về "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có thực sự xác định thời gian hỗ trợ liên quan đến các thành phần phần mềm có cập nhật như được mô tả trong "Thời gian Hỗ trợ" trong **IXIT 2-UserInfo** hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Việc truy cập thông tin công bố thời gian hỗ trợ cho người sử dụng tuân thủ mô tả trong **IXIT**;

• Việc truy cập thông tin công bố thời gian hỗ trợ không bị giới hạn;

• Thông tin về thời gian hỗ trợ đã được công bố.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu ở trên không đáp ứng.

3.3.7. Nhóm kiểm thử yêu cầu 2.3.7

3.3.7.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3.7, điều 2.3.7 Quy chuẩn này.

3.3.7.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với Model thiết bị.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá Model thiết bị camera có thể được nhận dạng một cách rõ ràng, thông qua việc gán nhãn trên thiết bị camera hoặc thông qua một giao diện vật lý theo "Model thiết bị" trong **IXIT 2-UserInfo**.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Định danh của thiết bị camera được nhận dạng rõ ràng thông qua việc gán nhãn trên thiết bị camera hoặc thông qua một giao diện vật lý.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.3.7.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc Model thiết bị camera.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc định danh của thiết bị camera có thể được nhận dạng bằng cách áp dụng phương pháp nhận dạng được mô tả trong "Model thiết bị" trong **IXIT 2-UserInfo** hay không.

b2) Phòng đo kiểm đánh giá liệu Model thiết bị thu được có sẵn dưới dạng văn bản đơn giản và có khớp với Model thiết bị được mô tả trong "Model thiết bị" trong **IXIT 2-UserInfo** hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Model thiết bị camera có thể được trích xuất theo cách nhận dạng được mô tả;
- Model thiết bị có sẵn dưới dạng văn bản đơn giản;
- Model thiết bị khớp với Model thiết bị trong **IXIT**.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.4. Lưu trữ các tham số an toàn nhạy cảm

3.4.1. Nhóm kiểm thử yêu cầu 2.4.1

3.4.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4.1, điều 2.4.1 Quy chuẩn này.

Nhóm kiểm thử này đánh giá liệu các tham số an toàn nhạy cảm có được lưu trữ an toàn theo loại của chúng bằng cách sử dụng các cơ chế bảo vệ được tuyên bố hay không. Tuy nhiên, đánh giá này không đảm bảo cho tính đầy đủ của các tham số an toàn nhạy cảm được mô tả ngoài sự nhất quán liên quan đến các **IXIT** khác.

CHÚ THÍCH: Mô hình hóa mối đe dọa, ví dụ được cung cấp bởi SO và mô hình tấn công cơ bản được mô tả trong **Phụ lục B.2**, rất hữu ích để đưa ra các đảm bảo an toàn phù hợp, đánh giá khái niệm các biện pháp bảo vệ tương ứng và đánh giá chức năng việc triển khai đúng đắn ở mức cơ bản.

3.4.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc lưu trữ an toàn các tham số an toàn nhạy cảm bao gồm các yêu cầu an toàn (i, ii, iii) và tính đầy đủ của tài liệu **IXIT**.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá các tuyên bố trong phần "Loại" của mỗi tham số an toàn nhạy cảm được cung cấp trong **IXIT 10-SecParam** có nhất quán với "mô tả" hay không.

b2) Phòng đo kiểm đánh giá liệu "Cam kết an toàn" của mỗi tham số an toàn nhạy cảm được cung cấp trong **IXIT 10-SecParam** có khớp với ít nhất các yêu cầu bảo vệ được chỉ định trong mục "Loại" hay không.

CHÚ THÍCH: Tham số an toàn quan trọng yêu cầu được bảo vệ về tính toàn vẹn và tính an toàn, trong khi tham số an toàn công khai chỉ yêu cầu bảo vệ về tính toàn vẹn.

b3) Phòng đo kiểm đánh giá liệu "Biện pháp bảo vệ" của mỗi tham số an toàn nhạy cảm được cung cấp trong **IXIT 10-SecParam** có đảm bảo các "Cam kết an toàn" đã được tuyên bố hay không.

CHÚ THÍCH: Xem xét việc sử dụng các bằng chứng bên ngoài để đáp ứng một phần yêu cầu nếu một yếu tố an toàn được sử dụng. Đối với việc sử dụng các bằng chứng bên ngoài, phòng đo kiểm sẽ xem xét các khía cạnh sau đây để đưa ra phán quyết **đáp ứng** cho nhóm thử nghiệm tương ứng mà không áp dụng các trường hợp thử nghiệm:

• Phạm vi của bằng chứng phải phù hợp với mục tiêu của nhóm thử nghiệm tương ứng;

• Mô tả về các hoạt động thử nghiệm là một phần của bằng chứng phải đáp ứng từng mục đích thử nghiệm bên trong nhóm thử nghiệm tương ứng;

• Độ sâu thử nghiệm tương ứng với mức độ đảm bảo đánh giá của bằng chứng phải phù hợp với mức độ tương ứng mà nhóm thử nghiệm giải quyết.

b4) Phòng đo kiểm đánh giá tính đầy đủ của các tham số an toàn nhạy cảm trong **IXIT 10-SecParam** bằng cách xem xét các tham số an toàn nhạy cảm trong thông tin được cung cấp trong tất cả các **IXIT** khác.

Ví dụ: Nếu có các cơ chế xác thực được mô tả trong **IXIT 1-AuthMech**, việc xác minh liệu các tham số mật mã tương ứng có được liệt kê trong **IXIT 10-SecParam** hữu ích để thu thập các chỉ dẫn.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với mọi tham số an toàn nhạy cảm, tuyên bố nhất quán với mô tả của nó;

• Đối với mọi tham số an toàn nhạy cảm, các Cam kết an toàn được yêu cầu đáp ứng các yêu cầu bảo vệ tối thiểu của chúng;

• Mỗi tham số an toàn nhạy cảm có cơ chế bảo vệ phù hợp cho các Cam kết an toàn được yêu cầu;

• Các tham số an toàn nhạy cảm được liệt kê đầy đủ.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu ở trên không đáp ứng.

3.4.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc lưu trữ an toàn các tham số an toàn nhạy cảm.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá tất cả các tham số an toàn nhạy cảm được cung cấp trong **IXIT 10-SecParam** có "Biện pháp bảo vệ" được triển khai theo tài liệu **IXIT** này hay không.

CHÚ THÍCH: Thông thường, trong khi kiểm tra thiết bị camera để thu thập các bằng chứng cho sự tồn tại và thực thi của cơ chế bảo vệ được mô tả cho một tham số an toàn nhạy cảm, có thể tìm thấy một chỉ báo cho sự không tuân thủ trong việc triển khai, nếu tồn tại ở mức cơ bản.

Ví dụ: Nếu thông tin về "Biện pháp bảo vệ" tuyên bố rằng một tham số an toàn nhạy cảm chỉ truy cập được đối với người sử dụng có đặc quyền và được bảo vệ bởi kiểm soát truy cập của hệ điều hành, thì việc cố gắng truy cập tham số qua các quy trình không có đặc quyền (ví dụ: thao tác đường dẫn qua các giao diện từ xa) hữu ích để thu thập các chỉ báo.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với mọi tham số an toàn nhạy cảm, việc triển khai cơ chế bảo vệ tương ứng tuân thủ theo tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.4.2. Nhóm kiểm thử yêu cầu 2.4.2

3.4.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4.2, điều 2.4.2 Quy chuẩn này.

Trong nhóm kiểm thử này, định danh duy nhất được mã hóa cứng trên mỗi thiết bị là một giá trị riêng biệt và tĩnh, đại diện cho thiết bị và các thông tin tiềm ẩn được mã hóa cứng mà giá trị dẫn xuất từ đó.

Nhóm kiểm thử này liên quan đến việc xác định các định danh được mã hóa cứng và xác định các yêu cầu bảo vệ thích hợp. Đánh giá cho việc lưu trữ chống giả mạo bằng bất kỳ phương tiện nào không phải là trọng tâm của kịch bản kiểm thử này.

CHÚ THÍCH 1: Đánh giá thiết kế các biện pháp bảo vệ chống giả mạo cho các định danh được mã hóa cứng và kiểm tra dấu hiệu về việc triển khai chính xác các biện pháp tương ứng là một phần của nhóm kiểm thử 2.4.1 theo cấu trúc. Tuy nhiên, các phương pháp thử nghiệm tương ứng được tham chiếu ở đây và có thể tối ưu hóa khi xây dựng kế hoạch thử nghiệm.

CHÚ THÍCH 2: Một định danh thiết bị dùng cho việc liên kết có thể được dẫn xuất từ một thông tin (có thể là một phần của thông tin bí mật) - tồn tại trong phần cứng. Thông tin này được coi là một phần định danh thiết bị.

3.4.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc lưu trữ chống giả mạo của các định danh mã hóa cứng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với mỗi tham số an toàn nhạy cảm trong **IXIT 10-SecParam** mà thông tin trong "Mô tả" cho thấy nó được sử dụng như một định danh mã hóa cứng, có một tuyên bố rõ ràng tương ứng được cung cấp.

b2) Phòng đo kiểm đánh giá liệu đối với mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam**, thông tin về "Cam kết an toàn" tương ứng có cung cấp khả năng chống giả mạo.

CHÚ THÍCH 1: Khả năng chống giả mạo đề cập đến bảo vệ chống lại các phương tiện như phương tiện vật lý, điện và phần mềm.

CHÚ THÍCH 2: Xem xét việc sử dụng bằng chứng bên ngoài (xem nội dung **CHÚ THÍCH** tại 3.4.1.2) để bao phủ một phần quy định nếu một yếu tố an toàn được sử dụng.

b3) Phòng đo kiểm đánh giá liệu "Biện pháp bảo vệ" của mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam** có cung cấp các "Cam kết an toàn" được yêu cầu liên quan đến khả năng chống giả mạo hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Bất kỳ định danh mã hóa cứng nào đều được tài liệu hóa tương ứng;

• Đối với tất cả các định danh mã hóa cứng, Cam kết an toàn đã bao gồm khả năng chống giả mạo;

• Mỗi định danh mã hóa cứng có một cơ chế bảo vệ cho khả năng chống giả mạo.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.4.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc lưu trữ chống giả mạo của các định danh mã hóa cứng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam**, các "Biện pháp bảo vệ" liên quan đến khả năng chống giả mạo được triển khai tuân thủ theo tài liệu **IXIT**.

CHÚ THÍCH: Thông thường, trong khi kiểm tra thiết bị camera để thu thập các bằng chứng cho sự tồn tại và thực thi của cơ chế bảo vệ được mô tả cho một tham số an toàn nhạy cảm, có thể tìm thấy một chỉ dẫn cho sự không tuân thủ của việc triển khai, nếu tồn tại ở mức cơ bản.

Ví dụ: Nếu "Biện pháp bảo vệ" tuyên bố rằng một định danh mã hóa cứng được bảo vệ chống giả mạo bằng một yếu tố an toàn, việc xác minh sự tồn tại và tích hợp đúng của yếu tố an toàn hữu ích để thu thập chỉ báo.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Đối với mọi định danh mã hóa cứng, việc triển khai bất kỳ cơ chế bảo vệ nào liên quan đến khả năng chống giả mạo tuân thủ tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.4.3. Nhóm kiểm thử yêu cầu 2.4.3

3.4.3.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4.3, điều 2.4.3 Quy chuẩn này.

Trong trường hợp này, một tham số được mã hóa cứng trong mã nguồn phần mềm của thiết bị là một giá trị tĩnh, được sử dụng chung cho mọi thiết bị mà mã nguồn phần mềm giống như thiết bị camera được triển khai.

Nhóm kiểm thử này đánh giá liệu có tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị không được tài liệu hóa trong các cơ chế cung cấp tham số an toàn quan trọng hay không. Bất cứ khi nào các tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị, đánh giá tập trung vào sự phù hợp của thiết kế và đánh giá chức năng của cơ chế cung cấp để đảm bảo rằng chúng không được sử dụng trong quá trình hoạt động của thiết bị camera. Cách tiếp cận này không thể cung cấp sự đảm bảo mạnh mẽ cho tính đầy đủ của tài liệu **IXIT** liên quan đến việc định danh các tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị.

Cần chú thích rằng cách tiếp cận này không loại trừ các cách tiếp cận bổ sung, ví dụ như các cách tiếp cận chủ động dựa trên việc quét phần mềm của thiết bị camera để tìm các mẫu nhúng khớp với các tham số an toàn quan trọng. Các cách tiếp cận bổ sung là theo quyết định của phòng đo kiểm.

CHÚ THÍCH: Các tham số an toàn công khai có thể được nhúng vào mã đối tượng trong phần mềm của thiết bị camera.

3.4.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các tham số an toàn quan trọng được mã hóa cứng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng được cung cấp trong **IXIT 10-SecParam** mà "Cơ chế cung cấp" chỉ ra rằng nó được mã hóa cứng trong mã nguồn phần mềm của thiết bị và được phản ánh trong "Mô tả" hay không.

b2) Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng trong **IXIT 10-SecParam**, mà được mã hóa cứng trong mã nguồn phần mềm của thiết bị theo "Mô tả", thông tin về "Cơ chế cung cấp" tương ứng có đảm bảo rằng nó không được sử dụng trong quá trình hoạt động của thiết bị camera hay không.

CHÚ THÍCH: Theo định nghĩa của tham số an toàn quan trọng trong Quy chuẩn này, việc tiết lộ hoặc sửa đổi một tham số như vậy làm suy yếu tính an toàn của thiết bị camera. Các tham số mà việc tiết lộ hoặc sửa đổi chỉ làm suy yếu các tài sản khác (ví dụ: tài sản trí tuệ) không được bao phủ bởi định nghĩa này.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Bất kỳ tham số an toàn quan trọng nào được mã hóa cứng trong mã nguồn phần mềm của thiết bị đều được tài liệu hóa;
- Đối với tất cả các tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị, "Cơ chế cung cấp" đảm bảo rằng nó không được sử dụng trong quá trình hoạt động của thiết bị camera.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.4.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các tham số an toàn quan trọng được mã hóa cứng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị được tài liệu hóa trong "Mô tả" của **IXIT 10-SecParam**, "Cơ chế cung cấp" có thực sự được áp dụng trong quá trình hoạt động của thiết bị camera hay không.

Ví dụ: Nếu một cơ chế cung cấp tuyên bố rằng một tham số an toàn quan trọng được mã hóa cứng được thay thế bởi người sử dụng sử dụng dữ liệu cá nhân (ví dụ: dựa trên mã QR), việc xác minh rằng người sử dụng được yêu cầu nhập dữ liệu này hữu ích để thu thập minh chứng.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Đối với tất cả các tham số an toàn quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị, việc áp dụng cơ chế cung cấp tuân thủ tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.4.4. Nhóm kiểm thử yêu cầu 2.4.4

3.4.4.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4.4, điều 2.4.4 Quy chuẩn này.

Nhóm kiểm thử này đánh giá các tài liệu đối với tất cả các tham số an toàn quan trọng được quy định cơ bản có được xác định và các cơ chế tạo ra chúng có đáp ứng các yêu cầu tương ứng hay không.

3.4.4.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các tham số an toàn quan trọng được sử dụng để kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm và cho việc bảo vệ giao tiếp với các dịch vụ liên kết liên quan đến các cơ chế tạo ra chúng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá tất cả các tham số an toàn quan trọng được cung cấp trong **IXIT 10-SecParam**, thông tin về "Mô tả" cho thấy rằng các tham số an toàn quan trọng được sử dụng để kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm hoặc để bảo vệ giao tiếp với các dịch vụ liên quan có được tài liệu hóa trong "Cơ chế khởi tạo" hay không.

b2) Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng được cung cấp trong **IXIT 10-SecParam**, thông tin về "Cơ chế khởi tạo" có đảm bảo rằng tham số an toàn quan trọng là duy nhất cho mỗi thiết bị và được tạo ra bằng một cơ chế giảm thiểu rủi ro của các cuộc tấn công tự động chống lại các nhóm thiết bị hay không.

CHÚ THÍCH 1: Bộ tạo số ngẫu nhiên được sử dụng để tạo tham số an toàn quan trọng đã được chứng nhận được xem như là một nguồn cung cấp đủ độ ngẫu nhiên (entropy).

CHÚ THÍCH 2: Các giải pháp tùy chỉnh (ví dụ: chưa được chứng nhận) cũng có thể cung cấp đủ độ ngẫu nhiên cho trường hợp sử dụng của thiết bị camera.

CHÚ THÍCH 3: Mức độ mà một cơ chế tạo ra được chấp nhận rộng rãi như là phù hợp cho một trường hợp sử dụng cụ thể phụ thuộc vào sự đồng thuận của cộng đồng chuyên môn trong lĩnh vực đó. Các cơ chế tạo ra được tiêu chuẩn hóa xếp hạng cao nhất, nhờ vào mức độ kiểm tra kỹ lưỡng mà chúng phải trải qua trong quá trình phát triển. Các tổ chức tiêu chuẩn hóa cung cấp các nguồn thông tin công khai về các cơ chế tạo phù hợp cho các bộ tạo bit ngẫu nhiên, dẫn xuất khóa, hàm băm an toàn. Về an toàn đầu-cuối và các cộng đồng mà các nhà sản xuất camera có thể quan tâm hơn, Mozilla® công khai danh sách các cấu hình cho TLS. Cuối cùng, có các danh mục công khai tham chiếu đến các tiêu chuẩn liên quan và các tiêu chuẩn quốc tế tương đương về độ dài khóa mật mã.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Tất cả các tham số an toàn quan trọng với mục đích trong phần "Mô tả" cho thấy rằng các tham số an toàn quan trọng được sử dụng để kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm hoặc để bảo vệ giao tiếp với các dịch vụ liên quan được tài liệu hóa trong "Cơ chế khởi tạo";

• Đối với tất cả các tham số an toàn quan trọng, "Cơ chế khởi tạo" đảm bảo rằng các tham số an toàn quan trọng là duy nhất cho mỗi thiết bị và được tạo ra bằng một cơ chế giảm thiểu rủi ro của các cuộc tấn công tự động chống lại các nhóm thiết bị.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.5. Quản lý kênh giao tiếp an toàn

3.5.1. Nhóm kiểm thử yêu cầu 2.5.1

3.5.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5.1, điều 2.5.1 Quy chuẩn này.

Mục tiêu của nhóm thử nghiệm này là đánh giá, trước tiên, liệu các phương pháp mã hóa có cung cấp các Cam kết an toàn cần thiết cho trường hợp sử dụng của giao tiếp

hay không và thứ hai, liệu các phương pháp mã hóa có dễ bị tấn công khả thi hay không.

3.5.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc phương pháp mã hóa sử dụng trong các kênh giao tiếp 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 tại thời điểm đánh giá.

b) Phương pháp đánh giá

b1) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá liệu "Cam kết an toàn" có phù hợp với trường hợp sử dụng của giao tiếp hay không.

b2) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá liệu cơ chế theo "mô tả" có phù hợp để đạt được "Cam kết an toàn" hay không.

CHÚ THÍCH 1: Một cách tiếp cận toàn diện là cần thiết để đánh giá mức độ an toàn của cơ chế truyền thông.

b3) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá liệu phương thức mã hóa có được coi là mật mã an toàn cho trường hợp sử dụng giao tiếp an toàn dựa trên một danh mục tham chiếu hay không. Nếu phương thức mã hóa không được bao gồm trong danh mục tham chiếu cho trường hợp sử dụng tương ứng (ví dụ: mật mã mới), nhà cung cấp sẽ cung cấp bằng chứng, ví dụ: một phân tích rủi ro, để biện minh cho rằng mật mã là phù hợp như mật mã an toàn cho trường hợp sử dụng. Trong trường hợp này, đánh giá liệu bằng chứng có phù hợp và đáng tin cậy cho trường hợp sử dụng hay không.

CHÚ THÍCH 2: Một danh sách các ví dụ về mật mã an toàn dựa trên trường hợp sử dụng được đưa ra trong ETSI TR 103 621 [3]. Ngoài ra, có các danh mục tham chiếu chung về mật mã an toàn, ví dụ: các cơ chế mật mã đã được SOGIS thống nhất (https://www.sogis.eu).

CHÚ THÍCH 3: Một thuật toán hoặc nguyên thủy mật mã bị ngừng sử dụng liên quan đến thuộc tính an toàn mong muốn hoặc dựa trên một tham số mật mã (ví dụ: kích thước khóa) không phù hợp, khi xem xét đến vòng đời dự kiến của thiết bị camera và khả năng linh hoạt về mật mã, không thể được coi là mật mã an toàn.

b4) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá liệu "phương thức mã hóa" không dễ bị tấn công khả thi đối với thuộc tính an toàn mong muốn trên cơ sở "Cam kết an toàn" bằng cách tham chiếu các báo cáo mật mã học.

CHÚ THÍCH 4: Các báo cáo phân tích mật mã đáng tin cậy thường được công bố trong tài liệu khoa học hoặc, thay vào đó, được cung cấp bởi SO. Thêm vào đó, điều khoản B.2 cung cấp thông tin về khả năng tấn công dự kiến ở mức độ cơ bản.

c) Kết luận đánh giá

c1) **Đáp ứng:** được đưa ra nếu đối với tất cả các cơ chế kết nối:

- Các Cam kết an toàn phù hợp với trường hợp sử dụng giao tiếp an toàn;
- Cơ chế phù hợp để đạt được các Cam kết an toàn liên quan đến trường hợp sử dụng;
- Tất cả các "phương thức mã hóa" được sử dụng được coi là mật mã an toàn cho trường hợp sử dụng;
- Tất cả các "phương thức mã hóa" được sử dụng không được biết là dễ bị tấn công khả thi đối với thuộc tính an toàn mong muốn.

c2) **Không đáp ứng:** nếu một trong các yêu cầu ở trên không đáp ứng.

3.5.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng về mật mã được sử dụng cho các cơ chế kết nối.

b) Phương pháp đánh giá

Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá chức năng liệu phương thức mã hóa đã được mô tả có được thiết bị camera sử dụng hay không.

Ví dụ 1: Sử dụng trình phân tích giao thức hoặc công cụ chặn gói tin.

Ví dụ 2: Nếu sử dụng giao tiếp an toàn TLS, việc thu thập kết nối TLS và so sánh các bộ mật mã đã sử dụng với mật mã được mô tả trong IXIT hữu ích để thu thập một chỉ báo.

Ví dụ 3: Nếu giao thức cho phép các chế độ an toàn khác nhau cho giao tiếp, cố gắng hạ cấp chế độ an toàn hữu ích để thu thập một chỉ báo.

c) Kết luận đánh giá

c1) **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng:

• Không có chỉ báo cho thấy bất kỳ cài đặt mật mã nào được sử dụng khác biệt so với mô tả trong tài liệu IXIT.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.5.2. Nhóm kiểm thử yêu cầu 2.5.2

3.5.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5.2, điều 2.5.2 Quy chuẩn này.

3.5.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng xác thực các đối tượng xác thực (người và máy); Chỉ cho phép cấu hình, sử dụng thiết bị camera khi đối tượng xác thực được xác thực thành công.

b) Phương pháp kiểm thử

Áp dụng tất cả các Phương pháp kiểm thử cho tất cả các trường hợp với sự hạn chế đối với các chức năng cho phép thay đổi liên quan đến an toàn theo "Cho phép cấu hình" trong **IXIT 13-SoftServ**. Các giao thức dịch vụ mạng được thiết bị camera sử dụng và vị trí nhà sản xuất không thể đảm bảo cấu hình cần thiết để thiết bị camera hoạt động sẽ được loại trừ.

b1) Đối với mỗi chức năng của thiết bị trong **IXIT 13-SoftServ** truy cập thông qua giao diện mạng trong trạng thái được khởi tạo theo "Mô tả", Phòng đo kiểm sẽ kiểm tra liệu có ít nhất phải tham chiếu một "Cơ chế Xác thực".

b2) Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá liệu cơ chế xác thực được mô tả trong **IXIT 1-AuthMech** có cho phép phân biệt giữa nhiều đối tượng xác thực khác nhau và từ chối các nỗ lực xác thực dựa trên định danh và/hoặc các yếu tố xác thực không hợp lệ hay không.

CHÚ THÍCH: Việc phân biệt thường được thực hiện dựa trên định danh duy nhất và/hoặc các yếu tố xác thực.

b3) Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá liệu các phương tiện bảo vệ cơ chế xác thực trong "phương thức

mã hóa" trong **IXIT 1-AuthMech** có cung cấp các "Cam kết an toàn" xác định cho cơ chế này và có khả năng chống lại các nỗ lực xâm phạm cơ chế hay không.

b4) Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá liệu quy trình ủy quyền được mô tả trong "Mô tả" trong **IXIT 1-AuthMech** có cho phép các đối tượng đã xác thực hợp lệ được cấp quyền truy cập và từ chối các đối tượng đã xác thực không hợp lệ hoặc các đối tượng chưa xác thực được cấp quyền truy cập hay không.

CHÚ THÍCH: Các giao thức dịch vụ mạng được thiết kế để cho phép cấu hình bên ngoài mà không cần xác thực, chẳng hạn như ARP, DHCP, DNS, ICMP và NTP sẽ không bắt buộc áp dụng quy định này.

c) Kết luận

c1) **Đáp ứng:** Nếu tất cả các yêu cầu dưới đây được đáp ứng, bao gồm:

- Ít nhất một cơ chế xác thực được tham chiếu cho mỗi chức năng của thiết bị truy cập thông qua giao diện mạng cho phép thay đổi liên quan đến an toàn;
- Mọi cơ chế xác thực cho phép phân biệt giữa nhiều đối tượng xác thực khác nhau và từ chối các nỗ lực xác thực dựa trên định danh và/hoặc các yếu tố xác thực không hợp lệ;
- Các phương tiện được sử dụng để bảo vệ một cơ chế xác thực cung cấp các Cam kết an toàn và có khả năng chống lại các nỗ lực xâm phạm cơ chế;
- Mọi cơ chế ủy quyền cho phép truy cập đối với các đối tượng đã xác thực với quyền truy cập hợp lệ;
- Mọi cơ chế ủy quyền từ chối truy cập đối với các đối tượng đã xác thực với quyền truy cập không hợp lệ và đối với các đối tượng chưa xác thực.

c2) **Không đáp ứng:** nếu một trong các yêu cầu ở trên không đáp ứng.

3.5.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của thiết bị cho phép thay đổi liên quan đến an toàn thông qua giao diện mạng liên quan đến xác thực và ủy quyền và tính đầy đủ của tài liệu **IXIT**.

b) Phương pháp kiểm thử

b1) Áp dụng tất cả các Phương pháp kiểm thử cho tất cả các trạng thái của Thiết bị camera với sự hạn chế đối với các chức năng cho phép thay đổi liên quan đến an toàn theo "Cho phép cấu hình" trong **IXIT 13-SoftServ**. Các giao thức dịch vụ mạng được Thiết bị camera sử dụng và nơi nhà sản xuất không thể đảm bảo cấu hình cần thiết để Thiết bị camera hoạt động sẽ được loại trừ.

- Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá chức năng xem một chủ thể chưa xác thực và một chủ thể có định danh hoặc thông tin xác thực không hợp lệ và một chủ thể đã xác thực không có quyền truy cập phù hợp có thể truy cập chức năng thiết bị ở trạng thái đã khởi tạo hay không.

CHÚ THÍCH: Về nguyên tắc, đơn vị thử nghiệm này không thể phân biệt giữa bước xác thực và bước ủy quyền việc triển khai nhằm mục đích giảm rò rỉ thông tin sẽ không tiết lộ bước nào sẽ không thành công đối với chủ thể.

- Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá chức năng xem một chủ thể đã xác thực có quyền truy cập phù hợp có thể truy cập chức năng thiết bị ở trạng thái đã khởi tạo hay không.

• Đối với mỗi "Cơ chế xác thực" được tham chiếu trong **IXIT 13-SoftServ**, Phòng đo kiểm sẽ đánh giá chức năng xem việc bảo vệ cơ chế xác thực có tuân thủ mô tả trong "Cam kết an toàn" và "Phương thức mã hóa" trong **IXIT 1-AuthMech** hay không.

CHÚ THÍCH: Các giao thức dịch vụ mạng được thiết kế để cho phép cấu hình bên ngoài mà không cần xác thực, chẳng hạn như DHCP, sẽ bị loại trừ trong bối cảnh quy định này.

b2) Đánh giá chức năng liệu các cơ chế kết nối không được tài liệu trong **IXIT 11-ComMech** có sẵn thông qua giao diện mạng trên thiết bị camera hay không.

Ví dụ: Các công cụ quét mạng cho phép phát hiện các cơ chế kết nối dựa trên mạng.

c) Kết luận

c1) **Đáp ứng:** Nếu tất cả các yêu cầu dưới đây được đáp ứng, bao gồm:

• Đối tượng chưa được xác thực, đối tượng có định danh hoặc thông tin đăng nhập không hợp lệ và đối tượng đã được xác thực nhưng không có quyền truy cập thích hợp không thể truy cập chức năng;
• Đối tượng đã được xác thực với quyền truy cập thích hợp truy cập chức năng của thiết bị;
• Không có dấu hiệu nào cho thấy cơ chế bảo vệ xác thực khác với tài liệu IXIT;
• Mọi cơ chế kết nối dựa trên mạng được phát hiện đều được tài liệu hóa trong IXIT.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu ở trên không đáp ứng.

3.5.3. Nhóm kiểm thử yêu cầu 2.5.3

3.5.3.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5.3, điều 2.5.3 Quy chuẩn này.

Trường hợp sử dụng trong quy định cơ bản được cụ thể hóa về việc truyền dẫn các tham số an toàn quan trọng qua các giao diện mạng truy cập từ xa, yêu cầu tối thiểu đảm bảo về tính an toàn.

Mục tiêu của nhóm kiểm thử này là đánh giá, trước tiên, liệu các phương pháp mã hoá có đảm bảo về tính an toàn cần thiết cho trường hợp truyền dẫn thông tin các tham số an toàn quan trọng hay không, và thứ hai, liệu các phương pháp mã hoá này có được biết là không khả thi để bị tấn công.

3.5.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với phương thức mã hoá được sử dụng để truyền dẫn tham số an toàn quan trọng qua giao diện mạng truy cập từ xa.

b) Phương pháp kiểm thử

b1) Đối với tất cả các "Cơ chế kết nối" được tham chiếu trong bất kỳ tham số an toàn quan trọng nào trong **IXIT 10-SecParam**, truy cập từ xa theo thông tin về "Mô tả" trong **IXIT 11-ComMech**, Phòng đo kiểm áp dụng tất cả các phương pháp kiểm thử được chỉ định, được yêu cầu đáp ứng tối thiểu về tính an toàn.

CHÚ THÍCH: Phương pháp kiểm thử được chỉ định bao gồm các bước thực hiện trong mục 3.5.1.2.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với tất cả các cơ chế kết nối được sử dụng để truyền dẫn các tham số an toàn quan trọng qua các giao diện mạng truy cập từ xa, bao gồm:

- Cam kết an toàn đáp ứng trường hợp sử dụng giao tiếp an toàn;
- Cơ chế phù hợp để đáp ứng Cam kết an toàn đối với trường hợp sử dụng;
- Phương thức mã hóa được coi là mật mã an toàn đối với trường hợp sử dụng;
- Phương thức mã hóa không được biết tới là rủi ro cho một cuộc tấn công.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.5.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với phương thức mã hoá được sử dụng để truyền dẫn các tham số an toàn quan trọng qua các giao diện mạng truy cập từ xa.

b) Phương pháp kiểm thử

b1) Đối với tất cả các "Cơ chế kết nối" được tham chiếu trong bất kỳ tham số an toàn quan trọng nào trong **IXIT 10-SecParam,** truy cập từ xa theo thông tin về "Mô tả" trong **IXIT 11-ComMech**, Phòng đo kiểm áp dụng tất cả các phương pháp kiểm thử được chỉ định.

CHÚ THÍCH: Phương pháp kiểm thử được chỉ định bao gồm các bước thực hiện trong 3.5.1.3.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Bất kỳ phương thức mã hoá nào được sử dụng tuân thủ tài liệu **IXIT** của nó.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.5.4. Nhóm kiểm thử yêu cầu 2.5.4

3.5.4.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5.4, điều 2.5.4 Quy chuẩn này.

3.5.4.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với quy trình quản lý an toàn liên quan tới vòng đời của các tham số an toàn quan trọng (b1) và đảm bảo các điều kiện tiên quyết cho việc thực hiện (b2).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu quy trình quản lý an toàn của các tham số an toàn quan trọng có bao phủ toàn bộ vòng đời của một tham số an toàn quan trọng, bao gồm:

- Khởi tạo;
- Cung cấp;
- Lưu trữ;
- Cập nhật;
- Ngừng hoạt động, lưu trữ và hủy bỏ;
- Các quy trình xử lý việc hết hạn và bị xâm phạm;

theo các quy trình trong **IXIT 14-SecMgmt**.

b2) Phòng đo kiểm đánh giá các "Xác nhận quản lý an toàn" trong **IXIT 4-Conf** có được tuân thủ.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Quản lý an toàn bao phủ toàn bộ vòng đời của một tham số an toàn quan trọng theo các quy trình của nó;

• Có một sự xác nhận cho việc thực hiện.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.6. Phòng chống tấn công thông qua các giao diện của thiết bị

3.6.1. Nhóm kiểm thử yêu cầu 2.6.1

3.6.1.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6.1, điều 2.6.1 Quy chuẩn này.

Về nguyên tắc, một giao diện logic được truy cập thông qua nhiều giao diện mạng: nhà sản xuất do đó đảm bảo rằng việc truy cập đến một giao diện logic đều được xác định. Nhà sản xuất vô hiệu hóa những giao diện mạng và logic không cần thiết để cung cấp chức năng của thiết bị, tùy thuộc vào mục đích của giao diện đó. Điều này đòi hỏi phải có kiến thức về nền tảng của họ và hiểu rõ các thành phần nào cung cấp giao diện mạng hoặc logic, và cách thức hoạt động của chúng. Điều này đặc biệt quan trọng khi tái sử dụng các nền tảng phần cứng và các thành phần từ các bên thứ ba.

3.6.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các giao diện mạng và logic của thiết bị camera.

b) Phương pháp kiểm thử

Đối với mỗi giao diện mạng và logic trong **IXIT 15-Intf** đang hoạt động theo thông tin về "Trạng thái", phòng đo kiểm đánh giá xem mục đích của giao diện trong "Mô tả" có hợp lệ cho việc được kích hoạt hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với mỗi giao diện mạng hoặc logic được đánh dấu là hoạt động trong tài liệu **IXIT**, có một mục đích hợp lệ cho việc giao diện đó được kích hoạt.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.6.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các giao diện mạng và logic của thiết bị camera (b1) và tính đầy đủ của tài liệu **IXIT** (b2).

b) Phương pháp kiểm thử

b1) Đối với mỗi giao diện mạng và logic trong **IXIT 15-Intf**, phòng đo kiểm đánh giá trạng thái hoạt động của giao diện có tuân thủ thông tin về "Trạng thái" trong tài liệu **IXIT** hay không.

CHÚ THÍCH: Một phương pháp sử dụng để phân tích một giao diện là sử dụng các công cụ kiểm thử giao thức trong môi trường hộp đen và suy luận từ thông tin thu được xem giao diện có được kích hoạt hay vô hiệu hóa trên thiết bị camera hay không. Đối với các trường hợp mà thiết bị camera cung cấp minh chứng (ví dụ: minh chứng trực quan của các đầu nối, ăng-ten và các thành phần) liệu giao diện có đang được kích hoạt hay không, kiểm tra khả năng truy cập cho phép xác nhận hoặc phủ định minh chứng đó.

b2) Phòng đo kiểm đánh giá chức năng xem các giao diện mạng hoặc logic không được mô tả trong **IXIT 15-Intf** có khả dụng qua một giao diện mạng trên thiết bị camera hay không.

Ví dụ: Các công cụ quét mạng cho phép phát hiện các giao diện mạng hoặc logic.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mỗi giao diện mạng hoặc logic được mô tả là vô hiệu trong tài liệu **IXIT** được xác nhận là vô hiệu hoặc không thể truy cập trên thiết bị camera;

• Mỗi giao diện mạng và logic được phát hiện đều được mô tả trong tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.6.2. Nhóm kiểm thử yêu cầu 2.6.2

3.6.2.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6.2, điều 2.6.2 Quy chuẩn này.

Nguyên tắc giảm thiểu áp dụng cho thông tin liên quan đến an toàn trong bối cảnh chưa xác thực yêu cầu rằng chỉ những thông tin cần thiết cho hoạt động của thiết bị hoặc dịch vụ trong bối cảnh chưa xác thực được tiết lộ. Cần chú thích rằng nhà sản xuất không thể giảm thiểu thông tin tiết lộ nếu có các yêu cầu phải tuân theo các giao thức tiêu chuẩn hóa như thiết kế, tiết lộ nhiều thông tin hơn mức cần thiết.

Ví dụ: Địa chỉ MAC trong Ethernet, Bluetooth® và Wi-Fi®, ARP, DNS.

3.6.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với thông tin được tiết lộ bởi các giao diện mạng mà không cần xác thực trong trạng thái khởi tạo.

b) Phương pháp kiểm thử

b1) Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, phòng đo kiểm đánh giá mô tả về "Thông tin được phép tiết lộ" được tiết lộ bởi các giao diện mà không cần xác thực trong trạng thái khởi tạo và được minh chứng là không ảnh hưởng đến tính an toàn có thực sự ảnh hưởng đến tính an toàn hay không.

b2) Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, phòng đo kiểm đánh giá mô tả về "Thông tin được phép tiết lộ" được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo và được chỉ ra là có liên quan đến an toàn có cần thiết cho hoạt động của thiết bị camera hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mọi giao diện mạng, bao gồm:

• Mỗi thông tin liên quan đến an toàn được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo đều được tài liệu hoá;

• Tất cả thông tin liên quan đến an toàn được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo đều cần thiết cho hoạt động của thiết bị camera.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.6.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với thông tin được tiết lộ bởi các giao diện mạng mà không cần xác thực trong trạng thái khởi tạo.

b) Phương pháp kiểm thử

Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, Phòng đo kiểm đánh giá liệu quan sát thông tin ảnh hưởng đến tính an toàn từ giao diện mà không cần xác thực trong trạng thái khởi tạo, mà không được mô tả trong phần "Thông tin được phép tiết lộ".

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với mọi giao diện mạng, chỉ quan sát được thông tin ảnh hưởng đến tính an toàn đã được mô tả trong tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.6.3. Nhóm kiểm thử yêu cầu 2.6.3

3.6.3.1. Mục tiêu kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6.3, điều 2.6.3 Quy chuẩn này.

Tại nhóm kiểm thử này, giao diện gỡ lỗi có thể bị vô hiệu hóa vĩnh viễn trong phần mềm hoặc, nếu dự kiến rằng nó hữu ích trong các trường hợp cụ thể tại vòng đời thiết bị, giao diện đó được kiểm soát bởi một cơ chế phần mềm đáng tin cậy. Xét đến mức độ an toàn được dự định trong quy chuẩn này, việc truy cập vật lý được định nghĩa là sử dụng dễ dàng với cáp giao diện tiêu chuẩn. Việc sử dụng các công cụ cụ thể để truy cập vật lý vào giao diện (chẳng hạn như đầu dò thử nghiệm) không nằm trong phạm vi đánh giá.

3.6.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các giao diện gỡ lỗi truy cập vật lý của thiết bị camera.

b) Phương pháp kiểm thử

b1) Đối với mỗi giao diện vật lý trong **IXIT 15-Intf** được mô tả là giao diện gỡ lỗi có thể truy cập theo thông tin về "Giao diện gỡ lỗi", phòng đo kiểm đánh giá các phương thức bảo vệ cho giao diện trong phần “Phương pháp bảo vệ” có bao gồm cơ chế phần mềm để vô hiệu hóa giao diện hay không.

b2) Đối với mỗi giao diện vật lý trong **IXIT 15-Intf** được mô tả là giao diện gỡ lỗi không được sử dụng liên tục theo “Mô tả”, kiểm tra xem giao diện có bị vô hiệu hóa vĩnh viễn theo thông tin về “Trạng thái” hay không.

b3) Đối với mỗi giao diện vật lý trong **IXIT 15-Intf** được mô tả là giao diện gỡ lỗi sử dụng trong trường hợp cụ thể theo “Mô tả”, kiểm tra xem giao diện có bị vô hiệu hóa mặc định theo thông tin về “Trạng thái” hay không.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Đối với mọi giao diện gỡ lỗi vật lý có thể truy cập, có một cơ chế phần mềm được mô tả để vô hiệu hóa giao diện;

• Đối với mọi giao diện gỡ lỗi vật lý không được sử dụng liên tục, giao diện bị vô hiệu hóa vĩnh viễn;

• Đối với mọi giao diện gỡ lỗi vật lý sử dụng trong trường hợp cụ thể, giao diện bị vô hiệu hóa theo mặc định.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.6.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các giao diện gỡ lỗi vật lý có thể truy cập của thiết bị camera (b1) và tính đầy đủ của tài liệu **IXIT** (b2).

b) Phương pháp kiểm thử

b1) Đối với mỗi giao diện vật lý có thể truy cập trên thiết bị camera được mô tả là "Giao diện gỡ lỗi" trong **IXIT 15-Intf**, Phòng đo kiểm đánh giá liệu giao diện có bị vô hiệu hóa hay không.

CHÚ THÍCH 1: Đối với bước kiểm thử này, đảm bảo rằng giao diện ở trạng thái mặc định của nó.

b2) Đối với mỗi giao diện vật lý có thể truy cập trên thiết bị camera, phòng đo kiểm đánh giá liệu giao diện có thể được sử dụng cho mục đích gỡ lỗi mặc dù nó không được mô tả là "Giao diện gỡ lỗi" trong **IXIT 15-Intf** hay không.

CHÚ THÍCH 2: Đối với bước kiểm thử này, thử sử dụng giao diện như một giao diện gỡ lỗi bằng cách sử dụng các phương pháp và công cụ tiêu chuẩn.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mọi giao diện gỡ lỗi vật lý có thể truy cập đều bị vô hiệu hóa;

• Mọi giao diện gỡ lỗi vật lý đều được tài liệu hoá trong tài liệu **IXIT**.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.7. Bảo vệ dữ liệu người sử dụng

3.7.1. Nhóm kiểm thử yêu cầu 2.7.1

3.7.1.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.7.1, điều 2.7.1 Quy chuẩn này.

Trường hợp sử dụng trong quy định này tập trung vào việc truyền dẫn dữ liệu cá nhân nhạy cảm giữa thiết bị và các dịch vụ liên quan, đảm bảo tối thiểu về tính an toàn.

Mục tiêu của nhóm kiểm thử này là đánh giá xem các phương pháp mã hóa có Cam kết an toàn cần thiết trong việc truyền dẫn dữ liệu cá nhân, và các phương pháp mã hóa đó không có rủi ro bị tấn công.

3.7.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với phương pháp mã hoá được sử dụng để truyền dẫn dữ liệu cá nhân nhạy cảm giữa thiết bị và các dịch vụ liên quan.

b) Phương pháp kiểm thử

Đối với tất cả "Cơ chế kết nối" trong bất kỳ dữ liệu cá nhân nhạy cảm nào trong **IXIT 21-PersData** theo thông tin về "Tính nhạy cảm" được tham chiếu trong **IXIT 11-ComMech**, nếu đối tác giao tiếp là một dịch vụ liên quan, phòng đo kiểm áp dụng tất cả các phương pháp kiểm thử được chỉ định trong 3.5.1.2 với đảm bảo tối thiểu về tính bảo mật.

CHÚ THÍCH: Trong trường hợp này, Cam kết an toàn về "tính bảo mật" có nghĩa là bảo vệ tính bảo mật trước các bên không được phép. Điều này bao gồm việc xác minh đối tác giao tiếp.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với tất cả các cơ chế kết nối được sử dụng để truyền dẫn dữ liệu cá nhân nhạy cảm giữa thiết bị và dịch vụ liên quan:

- Các "Cam kết an toàn" đáp ứng trường hợp truyền dẫn dữ liệu cá nhân nhạy cảm giữa thiết bị và dịch vụ liên quan;
- Cơ chế đáp ứng được các Cam kết an toàn đối với trường hợp sử dụng;
- Tất cả phương pháp mã hóa được sử dụng coi là Mạt mã an toàn đối với trường hợp sử dụng;
- Tất cả phương pháp mã hóa được sử dụng không được biết tới là dễ bị tấn công.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.7.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với phương pháp mã hóa được sử dụng để truyền dẫn dữ liệu cá nhân nhạy cảm giữa thiết bị và các dịch vụ liên quan.

b) Phương pháp kiểm thử

Đối với tất cả "Cơ chế kết nối" trong bất kỳ dữ liệu cá nhân nhạy cảm nào trong **IXIT 21-PersData** theo thông tin về "Tính nhạy cảm" được tham chiếu trong **IXIT 11-ComMech**, nếu đối tác giao tiếp là một dịch vụ liên quan, phòng đo kiểm áp dụng phương pháp kiểm thử được chỉ định trong 3.5.1.3.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Bất kỳ phương thức mã hóa được sử dụng tuân thủ tài liệu **IXIT** tương ứng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.7.2. Nhóm kiểm thử yêu cầu 2.7.2

3.7.2.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.7.2, điều 2.7.2 Quy chuẩn này.

Mục tiêu của nhóm kiểm thử này nhằm phát hiện bất kỳ khả năng nào của thiết bị camera để thu thập thông tin về môi trường xung quanh của nó, chẳng hạn như cảm biến quang học, âm thanh, sinh trắc học hoặc vị trí. Tất cả các khả năng này cần được

ghi lại một cách rõ ràng để người sử dụng biết về thông tin được thu thập bởi thiết bị camera.

CHÚ THÍCH 1: Mục tiêu là đảm bảo rằng không có khả năng cảm biến nào trong thiết bị camera mà chưa được tài liệu hóa. Các khả năng cảm biến không hoạt động có thể bị kẻ tấn công kích hoạt, ví dụ thông qua phần sụn bị xâm phạm. Nói chung, không phải tất cả các khả năng cảm biến của thiết bị đều nhất thiết phải hoạt động. Tuy nhiên, tất cả các khả năng cảm biến đều phải được tài liệu hóa.

CHÚ THÍCH 2: Sự rõ ràng và minh bạch của tài liệu đề cập đến việc mô tả dễ hiểu trong tài liệu, cũng như giải thích về sự hiện diện của các khả năng cảm biến trong thiết bị camera.

3.7.2.2. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các khả năng cảm biến bên ngoài (b1, b2) và tính đầy đủ của tài liệu **IXIT** (b3).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc truy cập tài liệu về các khả năng cảm biến bên ngoài như thông tin trong phần "Tài liệu mô tả về các cảm biến thiết bị camera sử dụng" trong **IXIT 2-UserInfo**.

b2) Phòng đo kiểm đánh giá tài liệu về các khả năng cảm biến bên ngoài như thông tin trong phần "Tài liệu mô tả về các cảm biến thiết bị camera sử dụng" trong **IXIT 2-UserInfo** có dễ hiểu đối với người sử dụng có kiến thức kỹ thuật hạn chế hay không (theo quy định tại **Phụ lục B.3**).

b3) Phòng đo kiểm đánh giá tất cả các khả năng cảm biến của thiết bị camera có được mô tả trong **IXIT 22-ExtSens** hay không.

CHÚ THÍCH: Bước kiểm thử này bao gồm kiểm tra trực quan vỏ bọc thiết bị camera để xác định các dấu hiệu của các khả năng cảm biến chưa được ghi lại. Nếu phát hiện có dấu hiệu, việc tháo bỏ vỏ bọc cung cấp sự trực quan.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Tài liệu truy cập được theo như mô tả trong **IXIT**;
- Tài liệu dễ hiểu đối với người sử dụng có kiến thức kỹ thuật hạn chế;
- Mỗi khả năng cảm biến của thiết bị camera đều được tài liệu hoá cho người sử dụng.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

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

3.8.1. Nhóm kiểm thử yêu cầu 2.8.1

3.8.1.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8.1, điều 2.8.1 Quy chuẩn này.

3.8.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với cơ chế khôi phục lại khi xảy ra sự cố về điện hoặc kết nối mạng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu sự kết hợp của các cơ chế khôi phục trong **IXIT 23-ResMech** có đáp ứng để bảo vệ trước sự cố mạng và mất điện theo mô tả trong "Cam kết an toàn".

b2) Đối với mỗi cơ chế khôi phục trong **IXIT 23-ResMech**, phòng đo kiểm đánh giá cơ chế đó theo thông tin về "Mô tả" có đáp ứng được "Cam kết an toàn".

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Các cơ chế khôi phục đáp ứng để bảo vệ trước sự cố mạng và mất điện;
- Mỗi cơ chế chống chịu đáp ứng được các Cam kết an toàn.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.8.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế khôi phục lại khi xảy ra sự cố về điện hoặc kết nối mạng.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm thử nghiệm việc ngắt kết nối mạng của thiết bị camera và đánh giá các cơ chế khôi phục có hoạt động như mô tả trong **IXIT 23-ResMech**.

b2) Phòng đo kiểm thử nghiệm việc ngắt nguồn cung cấp điện của thiết bị camera và đánh giá các cơ chế khôi phục có hoạt động như mô tả trong **IXIT 23-ResMech**.

Ví dụ: Nếu thiết bị camera giám sát các sự kiện cục bộ và báo cáo tới một dịch vụ liên quan qua giao diện mạng, việc ngắt kết nối mạng trong khi kích hoạt một sự kiện cục bộ và kiểm tra xem sau khi kết nối lại với mạng, sự kiện có hiển thị trên giao diện của dịch vụ liên quan hữu ích để thu thập một chỉ báo.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Hoạt động của các cơ chế khôi phục trong quá trình mất kết nối mạng và mất điện tuân thủ với tài liệu **IXIT** tương ứng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.8.2. Nhóm kiểm thử yêu cầu 2.8.2

3.8.2.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8.2, điều 2.8.2 Quy chuẩn này.

3.8.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế khôi phục lại khi xảy ra sự cố về điện hoặc kết nối mạng (b1), các hoạt động trong quá trình mất kết nối mạng (b2) và quá trình khôi phục sau khi gặp sự cố về điện (b3).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm áp dụng phương pháp kiểm thử được chỉ định trong 3.8.1.1 cho các cơ chế khôi phục được mô tả trong **IXIT 23-ResMech**.

b2) Phòng đo kiểm đánh giá các cơ chế khôi phục trong **IXIT 23-ResMech** bảo vệ trước sự cố kết nối mạng theo thông tin về "Loại" có đảm bảo thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ trong trường hợp mất kết nối mạng.

b3) Phòng đo kiểm đánh giá các cơ chế khôi phục trong **IXIT 23-ResMech** bảo vệ trước sự cố về điện theo thông tin về "Loại" có đảm bảo thiết bị camera khôi phục kết nối và chức năng sau khi mất điện trong trạng thái tương tự hoặc được cải thiện so với trước đó.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Các cơ chế khôi phục đáp ứng việc bảo vệ trước sự cố kết nối mạng và điện;
- Mỗi cơ chế khôi phục đáp ứng các Cam kết an toàn tương ứng;
- Các cơ chế khôi phục đảm bảo thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ trong trường hợp mất kết nối mạng;
- Các cơ chế khôi phục đảm bảo thiết bị camera khôi phục hoàn toàn sau khi mất điện.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.8.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế khôi phục lại khi xảy ra sự cố về điện hoặc kết nối mạng, các hoạt động trong quá trình mất kết nối mạng và quá trình khôi phục sau khi gặp sự cố về điện.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm thử nghiệm việc ngắt kết nối mạng của thiết bị camera và đánh giá các cơ chế chống chịu hoạt động như mô tả trong **IXIT 23-ResMech** và thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ sau khi mất kết nối mạng.

Ví dụ 1: Nếu thiết bị camera giám sát các sự kiện cục bộ và báo cáo chúng tới một dịch vụ liên quan qua giao diện mạng, việc ngắt kết nối mạng trong khi kích hoạt một sự kiện cục bộ và kiểm tra xem sau khi kết nối lại với mạng, sự kiện có hiển thị trên giao diện của dịch vụ liên quan hay không hữu ích để thu thập minh chứng.

b2) Phòng đo kiểm thử nghiệm việc ngắt nguồn cung cấp điện của thiết bị camera và đánh giá các cơ chế chống chịu hoạt động như mô tả trong **IXIT 23-ResMech** và thiết bị camera khôi phục kết nối và hoạt động trong trạng thái tương tự hoặc được cải thiện so với trước khi gặp sự cố về điện.

Ví dụ 2: Nếu thiết bị camera giám sát các sự kiện cục bộ và báo cáo chúng tới một dịch vụ liên quan qua mạng, kích hoạt một sự kiện cục bộ sau khi khôi phục nguồn điện và kiểm tra xem sự kiện có hiển thị trên giao diện của dịch vụ liên quan hay không hữu ích để thu thập minh chứng.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Hoạt động của các cơ chế chống chịu trong quá trình mất kết nối mạng hoặc mất điện tuân thủ tài liệu IXIT tương ứng;

• Thiết bị camera tiếp tục hoạt động và có thể hoạt động cục bộ sau khi mất kết nối mạng;

• Thiết bị camera khôi phục kết nối và chức năng sau khi gặp sự cố về điện trong trạng thái tương tự hoặc được cải thiện so với trước đó.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.8.3. Nhóm kiểm thử yêu cầu 2.8.3

3.8.3.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8.3, điều 2.8.3 Quy chuẩn này.

Nhóm kiểm thử này tập trung vào các khả năng sau:

• Thực hiện thiết lập kết nối theo tiêu chuẩn;

• Khả năng bảo vệ trước việc kết nối lại liên tục.

3.8.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các cơ chế khôi phục lại các cơ chế kết nối.

b) Phương pháp kiểm thử

b1) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, phòng đo kiểm đánh giá thông tin về "Biện pháp khôi phục" có phù hợp để đạt được kết nối với mạng một cách có trật tự, đồng thời xem xét bổ sung về khả năng của hạ tầng.

CHÚ THÍCH 1: Một biện pháp phù hợp để đạt được kết nối có trật tự là tuân thủ các tiêu chuẩn phù hợp về khởi tạo và kết thúc.

b2) Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, phòng đo kiểm đánh giá thông tin về "Biện pháp khôi phục" có phù hợp để hỗ trợ hoạt động kết nối mạng ổn định, đồng thời xem xét bổ sung về khả năng của hạ tầng.

CHÚ THÍCH 2: Một biện pháp phù hợp để hỗ trợ hoạt động kết nối mạng ổn định là ngăn chặn việc kết nối lại hàng loạt đồng thời. Điều này có thể được thực hiện bằng cách kết nối với một máy chủ ngẫu nhiên từ một danh sách cho sẵn (cân bằng tải) hoặc một độ trễ ngẫu nhiên khi kết nối lại.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Mỗi cơ chế kết nối cung cấp các biện pháp đáp ứng kết nối mạng một cách có trật tự;

• Mỗi cơ chế kết nối cung cấp các biện pháp đáp ứng hoạt động kết nối mạng ổn định.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.8.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các cơ chế khôi phục lại các cơ chế kết nối.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá việc triển khai các "Biện pháp khôi phục" cho mỗi "Cơ chế kết nối" trong **IXIT 11-ComMech** được thực hiện đúng như mô tả, đặc biệt xem xét bảo vệ trước việc kết nối lại hàng loạt đồng thời.

Ví dụ: Sử dụng một công cụ phát hiện lỗi hệ thống mạng để xác minh quá trình khởi tạo và kết thúc liên quan đến thiết lập kết nối tuân thủ các tiêu chuẩn tương ứng giúp thu thập các chỉ báo.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Hoạt động của bất kỳ biện pháp khôi phục nào đã triển khai tuân thủ tài liệu **IXIT** tương ứng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.9. Xoá dữ liệu trên thiết bị camera

3.9.1. Nhóm kiểm thử yêu cầu 2.9.1

3.9.1.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.9.1, điều 2.9.1 Quy chuẩn này.

3.9.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các chức năng xoá dữ liệu người sử dụng trên thiết bị camera.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá tồn tại ít nhất một chức năng được cung cấp theo **IXIT 25-DelFunc**, mà người sử dụng có thể thực hiện với kiến thức kỹ thuật hạn chế (xem **Phụ lục B.3**) theo thông tin về "Mô tả" và "Khởi tạo và tương tác" để xóa dữ liệu người sử dụng khỏi thiết bị đối với từng "Loại đối tượng".

b2) Phòng đo kiểm đánh giá mỗi chức năng trong **IXIT 25-DelFunc** có đủ khả năng xóa dữ liệu người sử dụng khỏi thiết bị.

CHÚ THÍCH 1: Việc xóa có thể được thực hiện bằng cách ghi đè với một giá trị được xác định trước hoặc bằng cách khóa vĩnh viễn quyền truy cập vào dữ liệu trên thiết bị.

b3) Phòng đo kiểm đánh giá các chức năng để xóa dữ liệu người sử dụng trong **IXIT 25-DelFunc** có bao gồm dữ liệu cá nhân, cấu hình người sử dụng và các giá trị mã hóa liên quan đến người sử dụng.

CHÚ THÍCH 2: Thông tin trong **IXIT 10-SecParam, IXIT 21-PersData** và các **IXIT** khác hữu ích để xác định dữ liệu người sử dụng.

CHÚ THÍCH 3: Giá trị mã hóa có thể là mật khẩu người sử dụng hoặc khóa.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu nếu không có dữ liệu người sử dụng nào được lưu trữ trên thiết bị; hoặc nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

• Tồn tại ít nhất một chức năng đơn giản được cung cấp cho người sử dụng để xóa dữ liệu người sử dụng khỏi thiết bị;

• Chức năng được mô tả đáp ứng đủ khả năng xóa dữ liệu người sử dụng khỏi thiết bị;

• Dữ liệu cá nhân, cấu hình người sử dụng và giá trị mã hóa được xóa bỏ với chức năng xóa dữ liệu người sử dụng khỏi thiết bị.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.9.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các chức năng xóa dữ liệu người sử dụng trên thiết bị camera.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm thử nghiệm tạo dữ liệu người sử dụng điển hình trên thiết bị camera liên quan đến việc sử dụng thiết bị.

CHÚ THÍCH: Dữ liệu này có thể là dữ liệu cá nhân, cấu hình người sử dụng hoặc giá trị mã hóa như mật khẩu hoặc khóa người sử dụng, khác với cấu hình tiêu chuẩn.

b2) Phòng đo kiểm thực hiện mỗi chức năng xóa dữ liệu người sử dụng khỏi thiết bị theo thông tin về "Loại đối tượng" trong **IXIT 25-DelFunc** và đánh giá mô tả về "Khởi tạo và tương tác" có tuân thủ **IXIT** không.

b3) Phòng đo kiểm thực hiện mỗi chức năng xóa dữ liệu người sử dụng khỏi thiết bị theo thông tin về "Loại đối tượng" trong **IXIT 25-DelFunc** và đánh giá dữ liệu người sử dụng có còn tồn tại sau khi hoàn thành thao tác không.

Ví dụ: Việc so sánh giữa cấu hình trước và sau khi xóa hữu ích để thu thập minh chứng dữ liệu người sử dụng chưa được xóa.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mỗi chức năng xóa dữ liệu người sử dụng khỏi thiết bị, bao gồm:

- Việc khởi tạo và tương tác của người sử dụng phù hợp với **IXIT**;
- Dữ liệu người sử dụng được xóa thành công.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.10. Xác thực dữ liệu đầu vào

3.10.1. Nhóm kiểm thử yêu cầu 2.10.1

3.10.1.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.10.1, điều 2.10.1 Quy chuẩn này.

Việc xác thực dữ liệu đầu vào đảm bảo rằng nơi nhận xử lý dữ liệu mà không gây ra hành vi không mong muốn. Điều này bao gồm việc xác minh rằng dữ liệu được cung cấp có đúng loại (định dạng dữ liệu và cấu trúc dữ liệu cho phép), có giá trị hợp lệ, có số lượng và thứ tự cho phép. Việc này có thể được thực hiện dựa trên danh sách giới hạn các giá trị được chấp nhận nếu danh sách này ngắn.

3.10.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các phương thức xác thực dữ liệu đầu vào của thiết bị camera.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá kết hợp các phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal** bao gồm tất cả các nguồn dữ liệu đầu vào như sau:

• Các giao diện người sử dụng, cho phép nhập dữ liệu đầu vào từ người sử dụng trong **IXIT 27-UserIntf**;

• Các giao diện lập trình ứng dụng (API), cho phép nhập dữ liệu đầu vào từ các nguồn bên ngoài trong **IXIT 28-ExtAPI**;

• Các kênh giao tiếp mạng, cho phép nhập dữ liệu đầu vào theo các phương pháp truyền dẫn từ xa tương ứng trong **IXIT 11-ComMech**.

b2) Đối với mỗi phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal**, phòng đo kiểm đánh giá hiệu quả trong việc xác thực dữ liệu đầu vào tương ứng.

CHÚ THÍCH: Việc xác thực thường bao gồm việc kiểm tra dữ liệu đầu vào có đúng định dạng và cấu trúc, giá trị hợp lệ, số lượng và thứ tự được phép nhằm ngăn chặn sự lợi dụng.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Các phương pháp xác thực dữ liệu đầu vào bao gồm dữ liệu đầu vào được nhập từ giao diện người sử dụng, truyền dẫn qua các API và các kết nối mạng giữa các dịch vụ và thiết bị;

• Mọi phương pháp xác thực dữ liệu đầu vào được mô tả đáp ứng hiệu quả trong việc xác thực dữ liệu đầu vào tương ứng.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.10.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các phương pháp xác thực dữ liệu đầu vào của thiết bị camera (b1) và tính đầy đủ của tài liệu **IXIT** (b2, b3).

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với mỗi phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal** ngăn chặn được việc xử lý dữ liệu đầu vào không mong muốn.

CHÚ THÍCH 1: Phòng đo kiểm tự lựa chọn một nguồn dữ liệu đầu vào cho mỗi phương pháp xác thực dữ liệu đầu vào.

CHÚ THÍCH 2: Phòng đo kiểm có thể sử dụng tất cả các thông tin xác thực của một người sử dụng để thử nghiệm sự lạm dụng.

CHÚ THÍCH 3: Các công cụ tự động được sử dụng để tạo ra dữ liệu không phù hợp với dữ liệu đầu vào dự kiến, ví dụ về định dạng và cấu trúc, giá trị, số lượng hoặc thứ tự.

Ví dụ 1: Nếu thiết bị camera sử dụng một giao diện với giao thức không có trạng thái, việc sử dụng một công cụ rà quét với đầu vào ngẫu nhiên để xác minh phương pháp xác thực dữ liệu đầu vào được mô tả hữu ích để thu thập minh chứng.

Ví dụ 2: Nếu thiết bị camera hỗ trợ giao diện trang trang thông tin điện tử, việc sử dụng công cụ quét ứng dụng trang thông tin điện tử để xác minh không có các vấn đề liên quan đến trang thông tin điện tử như XSS, SQL Injection, hoặc CSRF hữu ích để thu thập minh chứng.

b2) Phòng đo kiểm đánh giá đối với tất cả các giao diện người sử dụng của thiết bị camera có được mô tả trong **IXIT 27-UserIntf** theo tài liệu dành cho người sử dụng.

b3) Phòng đo kiểm đánh giá đối với tất cả các APIs truy cập từ xa của thiết bị camera có được mô tả trong **IXIT 28-ExtAPI**.

Ví dụ: Các công cụ quét mạng cho phép phát hiện các API truy cập từ xa.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Phương pháp xác thực dữ liệu đầu vào bảo vệ được việc xử lý dữ liệu đầu vào không mong muốn;

• Mọi giao diện người sử dụng được phát hiện đều được mô tả trong **IXIT**;

• Mọi API truy cập từ xa được phát hiện đều được mô tả trong **IXIT**.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.11. Bảo vệ dữ liệu trên thiết bị camera

3.11.1. Nhóm kiểm thử yêu cầu 2.11.1

3.11.1.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11.1, điều 2.11.1 Quy chuẩn này.

3.11.1.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với thông tin người sử dụng liên quan tới việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá liệu "Tài liệu về dữ liệu cá nhân" trong **IXIT 2-UserInfo** đáp ứng để người sử dụng được cung cấp thông tin về việc xử lý dữ liệu cá nhân.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

• Thông tin về việc xử lý dữ liệu cá nhân được cung cấp một cách hợp lý cho người sử dụng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.1.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với thông tin người sử dụng liên quan đến việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá đối với thông tin cung cấp về việc xử lý dữ liệu cá nhân (thông tin đã được thu thập) có tuân thủ theo mô tả trong "Tài liệu về dữ liệu cá nhân" trong **IXIT 2-UserInfo**.

b2) Phòng đo kiểm đánh giá đối với thông tin đã được thu thập về việc xử lý dữ liệu cá nhân khi truy cập vào "Tài liệu về dữ liệu cá nhân" trong **IXIT 2-UserInfo** có tuân thủ với mô tả trong "Quy trình xử lý" trong **IXIT 21-PersData**.

b3) Phòng đo kiểm đánh giá đối với thông tin đã được thu thập có mô tả những dữ liệu cá nhân nào đang được xử lý một cách dễ hiểu đối với người sử dụng có kiến thức kỹ thuật hạn chế (xem **Phụ lục B.3**).

b4) Phòng đo kiểm đánh giá đối với thông tin đã được thu thập có mô tả cách thức dữ liệu cá nhân đang được sử dụng, bởi ai, cho mục đích gì một cách dễ hiểu đối với người sử dụng có kiến thức kỹ thuật hạn chế (xem **Phụ lục B.3**).

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Thông tin về việc xử lý dữ liệu cá nhân được thu thập như mô tả;
- Thông tin đã được thu thập về việc xử lý dữ liệu cá nhân tuân thủ với mô tả của chúng;
- Dữ liệu cá nhân đang được xử lý được mô tả rõ ràng và minh bạch;
- Cách thức dữ liệu cá nhân đang được sử dụng, bởi ai, cho mục đích gì được mô tả rõ ràng và minh bạch.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.11.2. Nhóm kiểm thử yêu cầu 2.11.2

3.11.2.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11.2, điều 2.11.2 Quy chuẩn này.

Theo Quy chuẩn này, việc thu thập sự đồng ý "một cách hợp lệ" liên quan đến việc cung cấp cho người sử dụng một lựa chọn tham gia tự do, rõ ràng và minh bạch về việc liệu dữ liệu cá nhân của họ có được sử dụng cho một mục đích cụ thể hay không.

3.11.2.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với sự đồng ý của người sử dụng đối với việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở được sự đồng ý của người sử dụng theo thông tin về "Thu thập sự đồng ý", phòng đo kiểm đánh giá các lựa chọn đồng ý tham gia:

- Cho phép xác nhận một cách tự do;
- Các lựa chọn được đưa ra một cách rõ ràng;
- Các yêu cầu xác nhận phải minh bạch;

theo mô tả trong phần "Thu thập sự đồng ý".

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở được sự đồng ý của người sử dụng, bao gồm:

- Có mô tả về cách thức để thể hiện sự đồng ý (lựa chọn tham gia) đối với việc xử lý dữ liệu cá nhân cho các mục đích cụ thể;

• Lựa chọn đồng ý tham gia được đưa ra một cách tự do, rõ ràng và minh bạch.

c2) **Không đáp ứng:** Nếu một trong các yêu cầu trên không đáp ứng.

3.11.2.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với sự đồng ý của người sử dụng đối với việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở được sự đồng ý của người sử dụng theo thông tin về "Thu thập sự đồng ý", phòng đo kiểm đánh giá sự đồng ý của người sử dụng đối với việc xử lý dữ liệu cá nhân có được thu thập như mô tả trong **IXIT**.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở sự đồng ý của người sử dụng, bao gồm:

• Cách thức thu thập sự đồng ý của người sử dụng tuân thủ với mô tả.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.3. Nhóm kiểm thử yêu cầu 2.11.3

3.11.3.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11.3, điều 2.11.3 Quy chuẩn này.

Theo Quy chuẩn này, việc thu hồi sự đồng ý vào bất cứ thời điểm nào liên quan đến việc cấu hình thiết bị và chức năng dịch vụ một cách thích hợp.

3.11.3.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc thu hồi sự đồng ý của người sử dụng về việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở được sự đồng ý của người sử dụng theo thông tin về "Thu thập sự đồng ý", phòng đo kiểm đánh giá thông tin về "Thu hồi sự đồng ý" có mô tả cách thu hồi sự đồng ý đối với việc xử lý dữ liệu cá nhân vào bất cứ lúc nào bằng cách cấu hình thiết bị camera và chức năng dịch vụ một cách thích hợp.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở được sự đồng ý của người sử dụng, bao gồm:

• Cách thức thu hồi sự đồng ý đối với việc xử lý dữ liệu cá nhân vào bất cứ lúc nào được mô tả rõ ràng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.3.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc thu hồi sự đồng ý của người sử dụng về việc xử lý dữ liệu cá nhân.

b) Phương pháp kiểm thử

b1) Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở được sự đồng ý của người sử dụng theo thông tin về "Thu thập sự đồng ý", phòng đo kiểm đánh giá liệu sự đồng ý của người sử dụng đối với việc xử lý dữ liệu cá nhân được thu hồi như mô tả trong phần "Thu hồi sự đồng ý".

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở được sự đồng ý của người sử dụng, bao gồm:

- Cách thức thu hồi sự đồng ý của người sử dụng tuân thủ với mô tả.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.4. Nhóm kiểm thử yêu cầu 2.11.4

3.11.4.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11.4, điều 2.11.4 Quy chuẩn này.

3.11.4.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với đối với việc cung cấp thông tin cho người sử dụng liên quan đến việc xử lý dữ liệu đo đạc từ xa.

b) Phương pháp kiểm thử

i. Phòng đo kiểm đánh giá mô tả trong phần "Tài liệu về dữ liệu đo đạc từ xa" trong **IXIT 2-UserInfo** đáp ứng để người sử dụng nhận được thông tin về việc xử lý dữ liệu đo đạc từ xa.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Thông tin về việc xử lý dữ liệu đo đạc từ xa được cung cấp cho người sử dụng.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.4.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với đối với việc cung cấp thông tin cho người sử dụng liên quan đến xử lý dữ liệu đo đạc từ xa.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá thông tin cung cấp về việc xử lý dữ liệu đo đạc từ xa (thông tin được thu thập) tuân thủ mô tả trong phần "Tài liệu về dữ liệu đo đạc từ xa" trong **IXIT 2-UserInfo**.

b2) Phòng đo kiểm đánh giá thông tin về việc xử lý dữ liệu đo đạc từ xa thông qua việc truy cập "Tài liệu về dữ liệu đo đạc từ xa" trong **IXIT 2-UserInfo** có tuân thủ với "Mục đích" được mô tả trong **IXIT 24-TelData**.

b3) Phòng đo kiểm đánh giá thông tin về việc xử lý dữ liệu đo đạc từ xa có mô tả dữ liệu đo đạc từ xa nào đang được thu thập hay không.

b4) Phòng đo kiểm đánh giá thông tin về việc xử lý dữ liệu đo đạc từ xa có mô tả rõ ràng cách thức dữ liệu đo đạc từ xa được sử dụng, bởi ai và cho mục đích gì.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Thông tin về việc xử lý dữ liệu đo đạc từ xa được thu thập như mô tả;
- Thông tin về việc xử lý dữ liệu đo đạc từ xa tuân thủ với mô tả của chúng;
- Dữ liệu đo đạc từ xa đang được xử lý được mô tả rõ ràng và minh bạch;
- Cách thức dữ liệu đo đạc từ xa đang được sử dụng, bởi ai, cho mục đích gì được mô tả rõ ràng và minh bạch.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.5. Nhóm kiểm thử yêu cầu 2.11.5

3.11.5.1. Mục tiêu nhóm kiểm thử

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11.5, điều 2.11.5 Quy chuẩn này.

3.11.5.2. Đánh giá sự tuân thủ về thiết kế

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với việc thiết bị camera có tính năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

b) Phương pháp kiểm thử

b1) Đối với mỗi mô tả trong **IXIT 11-ComMech** và **IXIT 28-ExtAPI**, phòng đo kiểm đánh giá thiết bị camera có mô tả về các tính năng cho phép thiết lập cấu hình để thiết bị camera kết nối các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Có mô tả đầy đủ thông tin để minh chứng thiết bị camera có tính năng cho phép thiết lập cấu hình để thiết bị camera kết nối các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

3.11.5.3. Đánh giá sự tuân thủ về triển khai

a) Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc thiết bị camera có chức năng cho phép thiết lập cấu hình để thiết bị camera kết nối các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

b) Phương pháp kiểm thử

b1) Phòng đo kiểm đánh giá để minh chứng thiết bị camera kết nối các dịch vụ liên kết có chức năng cho phép thiết lập cấu hình để thiết bị camera và các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

b2) Phòng đo kiểm đánh giá để minh chứng các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam.

Ví dụ: Các công cụ rà quét mạng cho phép phát hiện các dịch vụ liên kết dựa trên giao diện mạng là hữu ích để thu thập minh chứng.

c) Kết luận

c1) **Đáp ứng:** Sản phẩm được đánh giá đáp ứng các yêu cầu, bao gồm:

- Minh chứng thiết bị camera khi sử dụng chức năng thiết lập cấu hình để thiết bị camera kết nối các dịch vụ liên kết lưu trữ dữ liệu tại Việt Nam thì sẽ chỉ kết nối đến các máy chủ đặt tại Việt Nam.

c2) **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

4. QUY ĐỊNH VỀ QUẢN LÝ

4.1. Thiết bị camera giám sát sử dụng giao thức Internet thuộc phạm vi điều chỉnh quy định tại 1.1 phải tuân thủ các yêu cầu kỹ thuật trong quy chuẩn này.

4.2. Chứng nhận, công bố hợp quy đối với các thiết bị thuộc phạm vi của Quy chuẩn này thực hiện theo quy định tại Thông tư quy định Danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông, phương thức đánh giá sự phù hợp theo 4.4 và các quy định hiện hành.

4.3. Phương tiện, thiết bị đo: Tuân thủ các quy định pháp luật về đo lường.

4.4. Phương thức đánh giá sự phù hợp

Thực hiện theo các phương thức: Phương thức 1, phương thức 5 và phương thức 7 được quy định tại Thông tư số 28/2012/TT-BKHCN và các sửa đổi, bổ sung, thay thế Thông tư số 28/2012/TT-BKHCN.

- Phương thức 1: Thử nghiệm mẫu điển hình.

Áp dụng để thực hiện cho sản phẩm, hàng hóa được sản xuất trong dây chuyền đã có chứng chỉ chứng nhận hệ thống quản lý chất lượng (ISO 9001 hoặc tương đương).

- Phương thức 5: Thử nghiệm mẫu điển hình và đánh giá quá trình sản xuất; giám sát thông qua thử nghiệm mẫu lấy tại nơi sản xuất hoặc trên thị trường kết hợp với đánh giá quá trình sản xuất.

Áp dụng để thực hiện cho sản phẩm, hàng hóa được sản xuất trong dây chuyền chưa có chứng chỉ chứng nhận hệ thống quản lý chất lượng (ISO 9001 hoặc tương đương) nhưng có quy trình sản xuất và giám sát đảm bảo chất lượng để đánh giá.

- Phương thức 7: Thử nghiệm, đánh giá lô sản phẩm, hàng hóa.

Áp dụng để thực hiện cho sản phẩm, hàng hóa không áp dụng được theo Phương thức 1 hoặc Phương thức 5.

5. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Các tổ chức, cá nhân liên quan có trách nhiệm thực hiện các quy định về chứng nhận và công bố hợp quy các thiết bị thuộc phạm vi của quy chuẩn này và chịu sự kiểm tra của cơ quan quản lý nhà nước theo các quy định hiện hành.

6. TỔ CHỨC THỰC HIỆN

6.1. Cục An toàn thông tin, Cục Viễn thông, Sở Thông tin và Truyền thông các địa phương có trách nhiệm tổ chức triển khai, hướng dẫn và quản lý các thiết bị camera giám sát sử dụng giao thức Internet theo quy chuẩn này.

6.2. Trong trường hợp các quy định nêu tại Quy chuẩn này có sự thay đổi, bổ sung hoặc được thay thế thì thực hiện theo quy định tại văn bản mới.

6.3. Trong quá trình triển khai thực hiện quy chuẩn này, nếu có vấn đề phát sinh, vướng mắc, các tổ chức và cá nhân có liên quan phản ánh bằng văn bản về Bộ Thông tin và Truyền thông (Vụ Khoa học và Công nghệ) để được hướng dẫn, giải quyết./.

Phụ lục A

(Quy định)

Danh mục thông tin phục vụ đánh giá

Bảng đối chiếu sử dụng nội dung IXIT

Các yêu cầu	Nội dung IXIT
2.1.1	IXIT 1-AuthMech: ID, Mô tả, Yếu tố xác thực, Cơ chế khởi tạo mật khẩu
2.1.2	IXIT 1-AuthMech: ID, Mô tả, Yếu tố xác thực, Cơ chế khởi tạo mật khẩu
2.1.3	IXIT 1-AuthMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa
2.1.4	IXIT 1-AuthMech: ID, Mô tả IXIT 2-UserInfo: Tài liệu hướng dẫn thay đổi thông tin xác thực
2.1.5	IXIT 1-AuthMech: ID, Mô tả, Ngăn chặn tấn công vét cạn
2.2.1	IXIT 2-UserInfo: Chính sách tiết lộ lỗ hổng
2.3.1	IXIT 7-UpdMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa, Khởi tạo và tương tác
2.3.2	IXIT 6-SoftComp: ID, Mô tả, Cơ chế cập nhật IXIT 7-UpdMech: ID, Mô tả, Khởi tạo và tương tác
2.3.3	IXIT 7-UpdMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa
2.3.4	IXIT 4-Conf: Xác nhận quy trình cập nhật IXIT 8-UpdProc: ID, Mô tả, Khung thời gian
2.3.5	IXIT 7-UpdMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa
2.3.6	IXIT 2-UserInfo: Thời gian hỗ trợ, Công bố thời gian hỗ trợ

2.3.7	IXIT 2-UserInfo: Model thiết bị
2.4.1	IXIT 10-SecParam: ID, Mô tả, Loại, Cam kết an toàn, Biện pháp bảo vệ
2.4.2	IXIT 10-SecParam: ID, Mô tả, Loại, Cam kết an toàn, Biện pháp bảo vệ
2.4.3	IXIT 10-SecParam: ID, Mô tả, Loại, Cơ chế cung cấp
2.4.4	IXIT 10-SecParam: ID, Mô tả, Loại, Cơ chế khởi tạo
2.5.1	IXIT 11-ComMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa
2.5.2	IXIT 1-AuthMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa IXIT 13-SoftServ: ID, Mô tả, Cho phép cấu hình, Cơ chế xác thực
2.5.3	IXIT 10-SecParam: ID, Mô tả, Loại, Cơ chế kết nối IXIT 11-ComMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa
2.5.4	IXIT 4-Conf: Xác nhận quản lý an toàn IXIT 14-SecMgmt: ID, Mô tả
2.6.1	IXIT 15-Intf: ID, Mô tả, Loại, Trạng thái
2.6.2	IXIT 15-Intf: ID, Mô tả, Loại, Thông tin được phép tiết lộ
2.6.3	IXIT 15-Intf: ID, Mô tả, Loại, Trạng thái, Giao diện gỡ lỗi, Phương pháp bảo vệ
2.7.1	IXIT 11-ComMech: ID, Mô tả, Cam kết an toàn, Phương thức mã hóa IXIT 21-PersData: ID, Mô tả, Quy trình xử lý, Cơ chế kết nối, Tính nhạy cảm
2.7.2	IXIT 2-UserInfo: Tài liệu về Cảm biến IXIT 22-ExtSens: ID, Mô tả
2.8.1	IXIT 23-ResMech: ID, Mô tả, Cam kết an toàn

2.8.2	IXIT 23-ResMech: ID, Mô tả, Loại, Cam kết an toàn
2.8.3	IXIT 11-ComMech: ID, Mô tả, Biện pháp khôi phục
2.9.1	IXIT 25-DelFunc: ID, Mô tả, Loại đối tượng, Khởi tạo và tương tác
2.10.1	IXIT 11-ComMech: ID, Mô tả IXIT 27-UserIntf: ID, Mô tả IXIT 28-ExtAPI: ID, Mô tả IXIT 29-InpVal: ID, Mô tả
2.11.1	IXIT 2-UserInfo: Tài liệu về dữ liệu cá nhân IXIT 21-PersData: ID, Mô tả, Quy trình xử lý
2.11.2	IXIT 21-PersData: ID, Mô tả, Thu thập sự đồng ý
2.11.3	IXIT 21-PersData: ID, Mô tả, Thu thập sự đồng ý, Thu hồi sự đồng ý
2.11.4	IXIT 2-UserInfo: Tài liệu về dữ liệu đo đạc từ xa IXIT 24-TelData: ID, Mô tả, Mục đích
2.11.5	IXIT 11-ComMech: ID, Mô tả IXIT 28-ExtAPI: ID, Mô tả

IXIT 1-AuthMech: Cơ chế xác thực

IXIT hoàn chỉnh liệt kê tất cả các cơ chế xác thực của thiết bị camera. Mẫu này bao gồm các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng một sơ đồ đánh số tuần tự hoặc một sơ đồ nhãn khác.

  Ví dụ: Đánh số tuần tự ("AuthMech-1") hoặc sơ đồ nhãn ("AuthMech-PswdTrang thông tin điện tửIf").

- **Mô tả**: Mô tả ngắn gọn về cơ chế xác thực và quy trình ủy quyền tương ứng. Cũng cần chỉ rõ liệu cơ chế này có được sử dụng cho xác thực người sử dụng hoặc xác thực giữa máy với máy và liệu nó được truy cập trực tiếp từ giao diện mạng hay không.
- **Yếu tố xác thực**: Loại thuộc tính được sử dụng để xác thực. Đối với mật khẩu, cần chỉ rõ thêm liệu mật khẩu có được người sử dụng đặt và sử dụng trong trạng thái đã khởi tạo hay không.

Ví dụ: Mật khẩu (do người sử dụng đặt), mật khẩu (cài sẵn), dấu vân tay sinh trắc học.

- **Cơ chế khởi tạo mật khẩu**: Nếu yếu tố xác thực là mật khẩu và không được đặt bởi người sử dụng: Mô tả cơ chế để tạo mật khẩu. Cũng cần chỉ rõ thêm liệu mật khẩu có duy nhất cho mỗi thiết bị và liệu nó có được cài sẵn hay không.

CHÚ THÍCH: Không cần phải có một đặc tả chi tiết về cơ chế tạo mật khẩu. Điều được coi là đủ khi mô tả giải thích các biện pháp đảm bảo rằng mật khẩu là duy nhất cho mỗi thiết bị trong bất kỳ trạng thái nào khác ngoài mặc định của nhà máy và giảm thiểu các rủi ro tấn công tự động dựa trên các quy luật hiển nhiên, chuỗi chung, thông tin công khai hoặc độ phức tạp không phù hợp khi được sử dụng làm mật khẩu cài sẵn và duy nhất cho mỗi thiết bị.

- **Cam kết an toàn**: Mô tả các mục tiêu an toàn đã được thực hiện và các mối đe dọa mà cơ chế này bảo vệ chống lại.

  Ví dụ: Các cơ chế xác thực rằng thực thể đã được xác thực đang sở hữu một mật khẩu hợp lệ. Bảo vệ tính bảo mật và toàn vẹn của mật khẩu trong quá trình truyền tải cũng được đảm bảo trong phiên làm việc.

- **Phương thức mã hóa**: Mô tả các phương pháp mã hóa (giao thức, hoạt động, nguyên thủy, chế độ và kích thước khóa) được sử dụng để bảo vệ cơ chế xác thực, xem xét việc quản lý khóa và thực hiện các "Cam kết an toàn" đã mô tả.

  Ví dụ: Xác thực được thực hiện qua khung xác thực http (IETF RFC 7235 [4]). Bảo vệ tính toàn vẹn và bảo mật của mật khẩu khi truyền tới thiết bị camera được thực hiện với bộ mã hóa TLS TLS_DHE_RSA_WITH_AES_128_CBC_SHA256.

- **Ngăn chặn tấn công vét cạn**: Nếu cơ chế xác thực có thể truy cập trực tiếp từ giao diện mạng: Mô tả phương pháp ngăn chặn kẻ tấn công từ việc tấn công vét cạn thông tin đăng nhập qua các giao diện mạng.

  Ví dụ: Thời gian trì hoãn 5 giây sau một lần đăng nhập không thành công trước khi tiếp tục đăng nhập lần tiếp theo.

IXIT 2-UserInfo: Thông tin cung cấp cho người sử dụng

IXIT hoàn chỉnh liệt kê các tài liệu, phiên bản và thông tin được cung cấp cho người sử dụng. Mẫu này chứa các mục sau, các mục này độc lập với nhau và thường được điền dưới dạng danh sách.

- **Tài liệu về Cơ chế Thay đổi**: Mô tả cách thức các cơ chế thay đổi giá trị xác thực được tài liệu hóa cho người sử dụng, bao gồm tất cả thông tin để truy cập tài liệu.

CHÚ THÍCH: Các cách tài liệu bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng, sổ tay hướng dẫn sử dụng hoặc trợ giúp tích hợp sẵn.

- **Tài liệu về Cảm biến**: Mô tả cách thức thông tin về khả năng cảm biến bên ngoài được tài liệu hóa cho người sử dụng, bao gồm tất cả thông tin để truy cập tài liệu.

CHÚ THÍCH: Các cách tài liệu bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng, sổ tay hướng dẫn sử dụng hoặc trợ giúp tích hợp sẵn.

- **Tài liệu về Dữ liệu Cá nhân**: Mô tả cách thức thông tin về xử lý dữ liệu cá nhân được tài liệu hóa cho người sử dụng, bao gồm tất cả thông tin để truy cập tài liệu.

CHÚ THÍCH: Các cách tài liệu bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng, sổ tay hướng dẫn sử dụng hoặc trợ giúp tích hợp sẵn.

- **Tài liệu về Dữ liệu đo đạc từ xa**: Mô tả cách thức thông tin về thu thập dữ liệu viễn thông được tài liệu hóa cho người sử dụng, bao gồm tất cả thông tin để truy cập tài liệu.

CHÚ THÍCH: Các cách tài liệu bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng, sổ tay hướng dẫn sử dụng hoặc trợ giúp tích hợp sẵn.

- **Model thiết bị**: Model của thiết bị camera và mô tả ngắn gọn về cách người sử dụng nhận biết model của thiết bị camera.

CHÚ THÍCH: Gọi API hoặc nhãn dán trên thiết bị camera là các tùy chọn để thông báo cho người sử dụng về Model.

- **Thời gian Hỗ trợ**: Thời gian trong đó sản phẩm hoặc dịch vụ được nhà sản xuất duy trì, ví dụ: về các bản cập nhật.
- **Công bố thời gian hỗ trợ**: Mô tả cách thức "Thời gian Hỗ trợ" được công bố và tài liệu hóa cho người sử dụng, bao gồm tất cả thông tin để truy cập công bố này.

CHÚ THÍCH: Cách công bố bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng.

- **Chính sách tiết lộ lỗ hổng**: Mô tả cách thức chính sách tiết lộ lỗ hổng được công bố, bao gồm tất cả thông tin để truy cập công bố này.

CHÚ THÍCH: Cách công bố bao gồm trang trang thông tin điện tử của nhà sản xuất và URL tương ứng.

IXIT 4-Conf: Cam kết

IXIT hoàn chỉnh liệt kê các xác nhận cho việc thiết lập các quy trình. Mẫu này chứa các mục sau, các mục này độc lập với nhau và thường được điền dưới dạng danh sách.

- **Xác nhận quy trình cập nhật (Có/Không)**: Xác nhận rằng đối với mỗi quy trình cập nhật được mô tả trong IXIT 8-UpdProc, cơ sở hạ tầng cần thiết đã được thiết lập và các nhà vận hành đã được đào tạo để đạt được "Khung thời gian" mục tiêu.
- **Xác nhận quản lý an toàn (Có/Không)**: Xác nhận rằng các quy trình quản lý an toàn được mô tả trong IXIT 14-SecMgmt đã được thiết lập.

IXIT 6-SoftComp: Các thành phần phần mềm

IXIT hoàn chỉnh liệt kê tất cả các thành phần phần mềm của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

CHÚ THÍCH: Mức độ chi tiết được sử dụng để chia phần mềm của thiết bị camera thành các thành phần phần mềm nhằm giúp phòng đo kiểm xác định các thành phần nào cập nhật và các thành phần nào không thể cập nhật.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác. **VÍ DỤ**: Đánh số tuần tự ("SoftComp-1") hoặc hệ thống nhãn ("SoftComp-Firmw").
- **Mô tả**: Mô tả ngắn gọn về thành phần phần mềm.

CHÚ THÍCH: BIOS, phần sụn và bộ nạp khởi động là các thành phần phần mềm có thể có của thiết bị camera.

- **Cơ chế cập nhật**: Tham chiếu đến các cơ chế cập nhật trong IXIT 7-UpdMech được sử dụng để cập nhật thành phần phần mềm. Danh sách rỗng của các cơ chế cập nhật cho thấy rằng không có cập nhật nào cho thành phần phần mềm và trong trường hợp này, cần cung cấp một lý do.

IXIT 7-UpdMech: Cơ chế cập nhật

IXIT hoàn chỉnh liệt kê tất cả các cơ chế cập nhật của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("UpdMech-1") hoặc hệ thống nhãn ("UpdMech-Firmw").

- **Mô tả**: Mô tả ngắn gọn về cơ chế cập nhật bao gồm các đặc điểm chính của nó. Ngoài ra, chỉ ra việc cung cấp một bản cập nhật có dựa trên mạng.

CHÚ THÍCH: Tùy thuộc vào độ phức tạp, hữu ích khi chia mô tả thành các bước trong đó cập nhật được thực hiện.

  Ví dụ: Bước cập nhật 1) Thiết bị camera truy vấn máy chủ X để xác minh xem có bản cập nhật nào không, được khởi xướng bởi người sử dụng; 2) Máy chủ cung cấp bản cập nhật cho thiết bị camera (dựa trên mạng); 3) Thiết bị camera xác minh tính xác thực và toàn vẹn của bản cập nhật; 4) Sau khi xác thực thành công, việc cài đặt bản cập nhật được thực hiện.

- **Cam kết an toàn**: Mô tả các mục tiêu an toàn đã được thực hiện và các mối đe dọa cơ chế bảo vệ. Đối với tính xác thực và toàn vẹn, cần chỉ ra liệu Cam kết an toàn được cung cấp bởi thiết bị camera hay không.

  Ví dụ: Cơ chế xác thực tính toàn vẹn và tính xác thực trước khi cài đặt bản cập nhật trên thiết bị camera.

- **Phương thức mã hóa**: Mô tả các phương pháp mã hóa (giao thức, hoạt động, nguyên thủy, chế độ và kích thước khóa) được sử dụng để bảo đảm cơ chế cập nhật với cân nhắc đến quản lý khóa và để hỗ trợ các "Cam kết an toàn" đã mô tả.

  Ví dụ: Tính xác thực và toàn vẹn của một bản cập nhật phần mềm được thực hiện bởi một gói phần sụn đã ký dựa trên IETF RFC 3852 [5]. Đối với chữ ký, SHA-256 với RSA 2048 và đệm PSS được sử dụng. Việc ký gói phần sụn được thực hiện với khóa riêng của nhà sản xuất. Khóa công khai để xác thực cập nhật được tích hợp trong quá trình sản xuất của thiết bị camera.

- **Khởi tạo và tương tác**: Mô tả ngắn gọn về quy trình cập nhật được khởi xướng và mô tả ngắn gọn về sự tương tác của người sử dụng, cần thiết để khởi động và áp dụng một bản cập nhật.

CHÚ THÍCH: Mục này cũng dùng để chỉ ra liệu đây có phải là cơ chế cập nhật tự động hay không.

IXIT 8-UpdProc: Quy trình cập nhật

IXIT hoàn chỉnh liệt kê các thủ tục của nhà sản xuất để quản lý các cập nhật an toàn. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác. **Ví dụ**: Đánh số tuần tự ("UpdProc-1") hoặc hệ thống nhãn ("UpdProc-SecUpd").
- **Mô tả**: Mô tả ngắn gọn về thủ tục triển khai các cập nhật an toàn bao gồm tất cả các thực thể và trách nhiệm liên quan.
- **Khung thời gian**: Khung thời gian mục tiêu để hoàn thành thủ tục.

IXIT 10-SecParam: Tham số an toàn

IXIT hoàn chỉnh liệt kê tất cả các tham số an toàn nhạy cảm (công khai và quan trọng) được lưu trữ một cách bền vững trên thiết bị camera trong quá trình sử dụng dự kiến. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("SecParam-1") hoặc hệ thống nhãn ("SecParam-Pswd").

- **Mô tả**: Mô tả ngắn gọn về tham số an toàn, bao gồm mục đích của nó. Ngoài ra, chỉ ra liệu thông số này có phải là mã định danh duy nhất được mã cứng cho mỗi thiết bị được sử dụng trong một thiết bị vì mục đích an toàn (mã định danh cứng) và/hoặc được mã cứng trong mã nguồn phần mềm thiết bị.

- **Loại**: Chỉ định liệu tham số an toàn là công khai hay quan trọng.

CHÚ THÍCH: Các tham số an toàn công khai và quan trọng được định nghĩa trong quy chuẩn này.

- **Cam kết an toàn**: Mô tả các mục tiêu an toàn cơ bản đã được thực hiện và các mối đe dọa mà tham số an toàn được bảo vệ chống lại trong quá trình lưu trữ ổn định.

- **Biện pháp bảo vệ**: Mô tả các biện pháp được áp dụng để đạt được các Cam kết an toàn. Điều này bao gồm các nguyên tắc và vai trò qua đó quyền truy cập vào thông số là có thể, bao gồm các quyền liên quan đến mỗi vai trò.

- **Cơ chế cung cấp**: Nếu mục "Loại" chỉ ra rằng thông số này là quan trọng: Mô tả cơ chế qua đó thông số được chỉ định giá trị của nó cho hoạt động của thiết bị camera.

CHÚ THÍCH:

- Việc chỉ định giá trị này có thể xảy ra trong quá trình khởi tạo hoặc trong trạng thái đã khởi tạo (ví dụ: khi chức năng của thiết bị dựa trên thông số này được kích hoạt bởi người sử dụng).

- Dữ liệu cấu hình bền vững, dữ liệu cấu hình thời gian chạy, đàm phán giao thức và chỉ định cho một giá trị mặc định là những cơ chế cung cấp có thể có.

- **Cơ chế kết nối**: Tham chiếu đến các Cơ chế kết nối trong IXIT 11-ComMech được sử dụng để giao tiếp thông số và một chỉ định liệu giao tiếp được thực hiện qua các giao diện truy cập từ xa hay không.

- **Cơ chế khởi tạo**: Nếu mục "Loại" chỉ ra rằng thông số này là quan trọng và được sử dụng cho các kiểm tra tính toàn vẹn và tính xác thực của các cập nhật phần mềm hoặc để bảo vệ kết nối với các dịch vụ liên quan: Mô tả cơ chế được sử dụng để tạo ra các giá trị của thông số và cũng cần chỉ ra rằng thông số này được sử dụng cho các kiểm tra tính toàn vẹn và tính xác thực của các cập nhật phần mềm hoặc để bảo vệ giao tiếp với các dịch vụ liên quan.

  Ví dụ: Tham chiếu đến một trình tạo số ngẫu nhiên chuẩn và các tài liệu thiết kế liên quan.

IXIT 11-ComMech: Cơ chế kết nối

IXIT hoàn chỉnh liệt kê tất cả các cơ chế kết nối của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("ComMech-1") hoặc hệ thống nhãn ("ComMech-IP").

- **Mô tả**: Mô tả ngắn gọn về cơ chế kết nối, bao gồm mục đích của nó và mô tả về giao thức được sử dụng. Đối với các giao thức chuẩn, chỉ cần tham chiếu là đủ. Ngoài ra, còn có chỉ định liệu cơ chế này truy cập từ xa hay không.

CHÚ THÍCH: Một cơ chế kết nối có thể là việc sử dụng Bluetooth®, WiFi® hoặc NFC để kết nối cục bộ giữa một ứng dụng di động và thiết bị camera.

- **Cam kết an toàn**: Mô tả các mục tiêu an toàn đã được thực hiện và các mối đe dọa mà cơ chế này được bảo vệ chống lại.

CHÚ THÍCH: Các Cam kết an toàn phổ biến nhất cần được xem xét bao gồm xác thực đối tác, xác thực nguồn gốc, bảo vệ tính toàn vẹn, bảo vệ tính bảo mật và chống phát lại.

- **Phương thức mã hóa**: Mô tả các phương pháp mã hóa (giao thức, hoạt động, sơ đồ, chế độ và kích thước khóa) được sử dụng để đảm bảo cơ chế kết nối có tính đến quản lý khóa và để hỗ trợ các " Cam kết an toàn " đã mô tả.

CHÚ THÍCH: Phương thức mã hóa bao gồm thông tin như: giao thức Z-Wave® với Security 2 Command Class v1 được sử dụng cho giao tiếp. Dữ liệu được chuyển giao được mã hóa xác thực với AES-128 CCM để bảo đảm tính bảo mật và toàn vẹn. Việc trao đổi khóa dựa trên một cơ chế ngoài băng.

- **Biện pháp khôi phục**: Mô tả các biện pháp để đảm bảo rằng việc thiết lập kết nối được thực hiện một cách có trật tự bao gồm một trạng thái vận hành ổn định và mong đợi để đạt được một kết nối ổn định.

CHÚ THÍCH: Các biện pháp phục hồi xem xét trình tự của giao thức được sử dụng, khả năng của cơ sở hạ tầng, việc đặt lại và khởi tạo giao thức và các vấn đề do việc kết nối lại hàng loạt gây ra.

IXIT 13-SoftServ: Dịch vụ phần mềm

IXIT hoàn chỉnh liệt kê tất cả các dịch vụ phần mềm của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("SoftServ-1") hoặc hệ thống nhãn ("SoftServ-Trang thông tin điện tửServ").

- **Mô tả**: Mô tả ngắn gọn về dịch vụ, bao gồm mục đích của nó. Ngoài ra còn có chỉ định liệu dịch vụ này có thể truy cập qua giao diện mạng hay không và liệu điều này có xảy ra ở trạng thái khởi tạo hay không.

CHÚ THÍCH: Một daemon SSH không được khởi động theo mặc định (bị tắt) vì nó chỉ được sử dụng cho mục đích phát triển là một ví dụ về dịch vụ này.

- **Cho phép cấu hình (Có/Không)**: Nếu dịch vụ có thể truy cập qua giao diện mạng: Chỉ định liệu dịch vụ có cho phép thay đổi cấu hình liên quan đến an toàn hay không và nếu có, mô tả ngắn gọn về cấu hình có thể.
- **Cơ chế xác thực**: Nếu dịch vụ có thể truy cập qua giao diện mạng: Tham chiếu đến các cơ chế xác thực trong IXIT 1-AuthMech được sử dụng để xác thực trước khi sử dụng dịch vụ.

IXIT 14-SecMgmt: Quy trình quản lý an toàn

IXIT hoàn chỉnh liệt kê tất cả các quy trình quản lý an toàn đối với các tham số an toàn quan trọng do SO triển khai cho thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

Ví dụ: Đánh số tuần tự ("SecMgmt-1") hoặc hệ thống nhãn ("SecMgmt-Passwd").

- **Mô tả**: Mô tả ngắn gọn về quy trình quản lý an toàn liên quan đến toàn bộ vòng đời của các tham số an toàn quan trọng. Nếu sử dụng tiêu chuẩn hiện có, cần tham chiếu đến tiêu chuẩn tương ứng.

CHÚ THÍCH: Vòng đời của các tham số an toàn quan trọng thường xem xét việc tạo ra, cung cấp, lưu trữ, cập nhật, ngừng hoạt động, lưu trữ lâu dài, phá hủy, và các quy trình xử lý việc hết hạn và tổn hại của thông số.

IXIT 15-Intf: Giao diện

IXIT hoàn chỉnh liệt kê tất cả các giao diện mạng, vật lý và logic của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("Intf-1") hoặc hệ thống nhãn ("Intf-LanPort").

- **Mô tả**: Mô tả ngắn gọn về giao diện, bao gồm mục đích của nó. Đối với các giao diện vật lý, cần mô tả thêm liệu giao diện này luôn cần thiết, không bao giờ cần thiết, hay chỉ cần thiết trong các trường hợp cụ thể (ví dụ: sử dụng gián đoạn), sau đó cần mô tả ngắn gọn về các trường hợp này.

- **Loại**: Chỉ định liệu giao diện này là mạng, vật lý (bao gồm cả giao diện không dây), logic, hay thuộc nhiều loại khác nhau.

CHÚ THÍCH: Các quy định của tiêu chuẩn này phân biệt giữa các giao diện mạng và logic, nhưng thường cả hai loại này đều tương đương. Do đó, trong trường hợp này, cả hai loại cần được chỉ định.

- **Trạng thái**: Chỉ định liệu giao diện có được bật hay tắt ở trạng thái khởi tạo. Đối với các giao diện được bật, cần có lý do.

- **Thông tin được phép tiết lộ**: Nếu giao diện là giao diện mạng: Mô tả thông tin được tiết lộ mà không cần xác thực ở trạng thái khởi tạo và lý do tiết lộ. Ngoài ra, cần chỉ định liệu thông tin này có liên quan đến an toàn hay không.

CHÚ THÍCH: Thông tin được tiết lộ có thể được sử dụng bởi kẻ tấn công để xác định một thiết bị dễ bị tổn thương, ví dụ như phiên bản phần mềm.

- **Giao diện gỡ lỗi**: Nếu giao diện là giao diện vật lý: Chỉ định liệu giao diện này có thể được sử dụng như giao diện gỡ lỗi hay không.

- **Phương pháp bảo vệ**: Nếu giao diện là giao diện vật lý: Mô tả các phương pháp bảo vệ cần thiết để hạn chế việc tiếp xúc của giao diện này.

CHÚ THÍCH :

- Đối với các giao diện gỡ lỗi, cần có mô tả về cơ chế phần mềm được sử dụng để vô hiệu hóa giao diện (xem 3.6.3).

- Đối với các giao diện không phải là giao diện vô tuyến, vỏ thiết bị là một phương pháp bảo vệ.

IXIT 21-PersData: Dữ liệu cá nhân

IXIT hoàn chỉnh liệt kê tất cả các dữ liệu cá nhân được xử lý bởi thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("PersData-1") hoặc hệ thống nhãn ("PersData-PayInfo").

- **Mô tả**: Mô tả ngắn gọn về loại dữ liệu cá nhân được thiết bị camera xử lý.

  Ví dụ: Dữ liệu nhật ký về việc sử dụng thiết bị camera, thông tin thanh toán, dữ liệu vị trí có dấu thời gian, luồng âm thanh đầu vào hoặc dữ liệu sinh trắc học.

CHÚ THÍCH:

- Theo Quy chuẩn này, dữ liệu cá nhân là bất kỳ thông tin nào liên quan đến định danh hoặc có thể định danh được một cá nhân .

- Các loại dữ liệu cá nhân cần được mô tả ở mức độ chi tiết cung cấp sự hiểu biết tổng quát về loại dữ liệu đang được xử lý. Điều này bao gồm sự hiểu biết tổng quát về mức độ nhạy cảm của dữ liệu cá nhân phù hợp với thuật ngữ nổi tiếng.

- **Quy trình xử lý**: Mô tả cách thức dữ liệu cá nhân được xử lý, bao gồm tất cả các bên liên quan. Ngoài ra, cũng được mô tả mục đích của việc xử lý.

CHÚ THÍCH: Lưu trữ vĩnh viễn dữ liệu cá nhân, bao gồm cả sao lưu, là một hoạt động xử lý.

- **Cơ chế kết nối**: Tham chiếu đến các cơ chế kết nối trong IXIT 11-ComMech được sử dụng để giao tiếp dữ liệu cá nhân và chỉ định xem đối tác giao tiếp có phải là dịch vụ liên kết hay không (Có/Không). Một danh sách Cơ chế kết nối rỗng cho thấy rằng dữ liệu cá nhân không được truyền tải.
- **Tính nhạy cảm (Có/Không)**: Chỉ định xem dữ liệu cá nhân có tính nhạy cảm theo định nghĩa trong yêu cầu 2.7-1 trong quy chuẩn này hay không.
- **Thu thập sự đồng ý**: Nếu dữ liệu cá nhân được xử lý trên cơ sở sự đồng ý của người sử dụng: Mô tả cách thức thu thập sự đồng ý cho việc xử lý từ người sử dụng.
- **Thu hồi sự đồng ý**: Nếu dữ liệu cá nhân được xử lý trên cơ sở sự đồng ý của người sử dụng: Mô tả cách thức người sử dụng thu hồi sự đồng ý cho việc xử lý dữ liệu cá nhân.

IXIT 22-ExtSens: Cảm biến bên ngoài

IXIT hoàn chỉnh liệt kê tất cả các khả năng cảm biến bên ngoài của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("ExtSens-1") hoặc hệ thống nhãn ("ExtSens-Cam").

- **Mô tả**: Mô tả ngắn gọn về khả năng cảm biến.

IXIT 23-ResMech: Cơ chế khôi phục sau sự cố

IXIT hoàn chỉnh liệt kê tất cả các cơ chế phục hồi cho kết nối mạng và mất điện của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("ResMech-1") hoặc hệ thống nhãn ("ResMech-Power").

- **Mô tả**: Mô tả cơ chế góp phần vào khả năng phục hồi của thiết bị camera đối với sự cố kết nối mạng và/hoặc mất điện.

CHÚ THÍCH:

- Một cơ chế phục hồi như vậy có thể là cơ chế ghi nhật ký trên hệ thống tệp ext4, bảo vệ tính toàn vẹn của hệ thống tệp trong trường hợp mất điện.

- Một cơ chế phục hồi như vậy có thể là một viên pin nhỏ cho phép tắt thiết bị khẩn cấp an toàn (pin dự phòng). Nó bảo vệ chống mất dữ liệu trong trường hợp mất điện.

- **Loại**: Chỉ định xem cơ chế phục hồi liên quan đến kết nối mạng hay mất điện hoặc cả hai.
- **Cam kết an toàn**: Mô tả các mục tiêu an toàn được hiện thực hóa và các mối đe dọa cơ chế bảo vệ.

  Ví dụ: Cơ chế bảo vệ tính toàn vẹn dữ liệu của thiết bị camera trong trường hợp mất điện.

IXIT 24-TelData: Dữ liệu đo đạc từ xa

IXIT hoàn chỉnh liệt kê tất cả dữ liệu đo đạc từ xa được thu thập bởi thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("TelData-1") hoặc hệ thống nhãn ("TelData-CrashLog").
- **Mô tả**: Mô tả ngắn gọn về dữ liệu đo đạc từ xa được thu thập và cung cấp cho nhà sản xuất bởi thiết bị camera.
- **Mục đích**: Mô tả ngắn gọn về mục đích thu thập dữ liệu.

IXIT 25-DelFunc: Chức năng xóa dữ liệu

IXIT hoàn chỉnh liệt kê tất cả các chức năng xóa dữ liệu của người sử dụng. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("DelFunc-1") hoặc hệ thống nhãn ("DelFunc-CloudServ").
- **Mô tả**: Mô tả ngắn gọn về chức năng dùng để xóa dữ liệu của người sử dụng. Nếu "Loại đối tượng" chỉ ra rằng một dịch vụ liên kết được đề cập: Dịch vụ liên kết liên quan được bảo đảm bởi chức năng sẽ được chỉ định thêm.

CHÚ THÍCH: Cài đặt của thiết bị camera có thể cung cấp một chức năng để xóa dữ liệu cá nhân từ một máy chủ đám mây.

- **Loại đối tượng**: Chỉ ra liệu chức năng này có liên quan đến dữ liệu người sử dụng trên thiết bị hoặc dữ liệu cá nhân trên các dịch vụ liên kết hoặc cả hai.
- **Khởi tạo và tương tác**: Mô tả ngắn gọn về tương tác của người sử dụng, điều cần thiết để khởi tạo và áp dụng chức năng xóa.

IXIT 27-UserIntf: Giao diện người sử dụng

IXIT hoàn chỉnh liệt kê tất cả các giao diện người sử dụng của thiết bị camera, cho phép nhập liệu từ người sử dụng. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("UserIntf-1") hoặc hệ thống nhãn ("UserIntf-Config").
- **Mô tả**: Mô tả ngắn gọn về giao diện người sử dụng cho phép nhập liệu từ người sử dụng và cũng chỉ ra cách người sử dụng truy cập giao diện này.

IXIT 28-ExtAPI: Giao diện lập trình ứng dụng (API) bên ngoài

IXIT hoàn chỉnh liệt kê tất cả các API của thiết bị camera, cho phép nhập liệu từ các nguồn bên ngoài. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  Ví dụ: Đánh số tuần tự ("ExtAPI-1") hoặc hệ thống nhãn ("ExtAPI-SOAP-Cloud").

- **Mô tả**: Mô tả về API cho phép nhập liệu từ các nguồn bên ngoài của thiết bị camera.

CHÚ THÍCH: Các API bên ngoài thường được sử dụng cho giao tiếp giữa máy với máy.

IXIT 29-InpVal: Xác nhận đầu vào dữ liệu

IXIT hoàn chỉnh liệt kê tất cả các phương pháp xác thực đầu vào dữ liệu của thiết bị camera. Mẫu này chứa các mục sau và thường được điền dưới dạng bảng.

- **ID**: Mã định danh duy nhất cho mỗi IXIT, được chỉ định bằng cách sử dụng sơ đồ đánh số tuần tự hoặc một số hệ thống nhãn khác.

  VÍ DỤ: Đánh số tuần tự ("InpVal-1") hoặc hệ thống nhãn ("InpVal-NetwCom").

- **Mô tả**: Mô tả phương pháp xác thực đầu vào dữ liệu qua giao diện người sử dụng hoặc chuyển qua các API và giữa các mạng trong các dịch vụ và thiết bị bao gồm cách xử lý dữ liệu không mong muốn. Ngoài ra, cũng chỉ ra những nguồn dữ liệu nào được phương pháp này xử lý.

CHÚ THÍCH: Để xác thực đầu vào dữ liệu, có thể kiểm tra xem liệu dữ liệu có thuộc loại cho phép (định dạng và cấu trúc), có giá trị cho phép, có số lượng cho phép hoặc có thứ tự cho phép hay không.

Phụ lục B

(Tham khảo)

Thông tin đánh giá bổ sung

B.1. Mô hình đe dọa

Mô hình đe dọa được công nhận rộng rãi là một trong những hoạt động quan trọng nhất trong an toàn hệ thống thông tin. Mô hình đe dọa cung cấp thông tin cho việc phát hiện các hành động và trình tự của chúng mà một tác nhân độc hại có thể thực hiện nhằm làm suy yếu, gây thiệt hại hoặc làm tổn hại đến giá trị của một hệ thống thông tin.

Mô hình đe dọa liên quan đến việc phát triển và áp dụng có kỷ luật một biểu diễn về các mối đe dọa đối kháng, tức là các nguồn, kịch bản và sự kiện cụ thể đối với chúng. Các mối đe dọa như vậy có thể nhắm mục tiêu hoặc ảnh hưởng đến một tài sản, đó có thể là một thiết bị, một ứng dụng, một hệ thống, một mạng, một chức năng kinh doanh (và các hệ thống hỗ trợ tương ứng), hoặc bất kỳ tài sản nào khác được định nghĩa trong phạm vi quan tâm.

Như bất kỳ mô hình nào, mô hình đe dọa là một biểu diễn trừu tượng của miền liên quan đến các mối đe dọa và các mối quan tâm chính liên quan đến những mối đe dọa đó. Trong khía cạnh này, mô hình đe dọa được sử dụng để nắm bắt kiến thức một cách có cấu trúc, cung cấp một ngôn ngữ chung hỗ trợ cho việc thảo luận về kiến thức đó và thực hiện các phân tích và suy luận trong lĩnh vực tương ứng.

Các khái niệm chính của một mô hình đe dọa bao gồm sự kiện đe dọa, nguồn đe dọa, kịch bản đe dọa và hậu quả.

Các mối đe dọa là những sự kiện gây hại đến tính bảo mật, tính toàn vẹn hoặc tính sẵn sàng của thông tin hoặc hệ thống thông tin, thông qua việc tiết lộ, lạm dụng, thay đổi hoặc hủy hoại trái phép thông tin hoặc hệ thống thông tin. Theo ISO/IEC 15408 [6], một mối đe dọa là nguyên nhân tiềm tàng của một sự cố gây hại cho một hệ thống hoặc tổ chức. Một mối đe dọa bao gồm một tài sản, một tác nhân đe dọa và một hành động bất lợi của tác nhân đe dọa đối với tài sản đó.

Hơn nữa, một mối đe dọa được thực hiện bởi một tác nhân đe dọa và dẫn đến một sự cố không mong muốn phá vỡ các mục tiêu an toàn nhất định đã được định nghĩa trước.

Một sự kiện đe dọa là một tình huống có khả năng gây ra hậu quả không mong muốn hoặc tác động lên một mẩu thông tin cụ thể, một tập hợp các hệ thống thông tin cụ thể hoặc cả hai.

Một kịch bản đe dọa là một tập hợp các sự kiện đe dọa riêng biệt, liên quan đến một tập hợp nguồn đe dọa cụ thể, và được sắp xếp theo thời gian.

Có nhiều phương pháp và kỹ thuật khác nhau để xây dựng mô hình đe dọa. Các Tiêu chí Chung (CC) cho sự đảm bảo và đánh giá an toàn được định nghĩa trong ISO/IEC 15408 [6] là một phương pháp được thiết lập.

Phân tích Đe dọa, Lỗ hổng và Rủi ro (TVRA) là một phương pháp tiêu chuẩn khác được sử dụng để phát triển mô hình đe dọa. Phân tích Đe dọa, Lỗ hổng và Rủi ro (TVRA) tuân theo một cách tiếp cận có cấu trúc thông qua các bước sau:

1. Xác định Đích Đánh giá (TOE) dẫn đến mô tả cấp cao về các tài sản chính của TOE và môi trường TOE và một đặc tả về mục tiêu, mục đích và phạm vi của TVRA.
2. Xác định các mục tiêu dẫn đến một tuyên bố cấp cao về các mục tiêu an toàn và các vấn đề cần giải quyết.
3. Xác định các yêu cầu an toàn chức năng, được rút ra từ các mục tiêu từ bước 2.
4. Kiểm kê các tài sản như các tinh chỉnh của mô tả tài sản cấp cao từ bước 1 và các tài sản bổ sung do kết quả của các bước 2 và 3.
5. Xác định và phân loại các lỗ hổng trong hệ thống, các mối đe dọa có khả năng khai thác chúng và các sự cố không mong muốn xảy ra.
6. Định lượng khả năng xảy ra và tác động của các mối đe dọa.
7. Thiết lập các rủi ro.
8. Xác định khung biện pháp đối phó (thiết kế) dẫn đến danh sách các dịch vụ và khả năng an toàn thay thế cần thiết để giảm thiểu rủi ro.
9. Phân tích chi phí và lợi ích của các biện pháp đối phó (bao gồm phân tích chi phí và lợi ích của các yêu cầu an toàn tùy thuộc vào phạm vi và mục đích của TVRA) để xác định các dịch vụ và khả năng bảo mật phù hợp nhất trong số các phương án thay thế từ bước 8.
10. Đặc tả các yêu cầu chi tiết cho các dịch vụ và khả năng an toàn từ bước 9.

B.2. Mô hình kẻ tấn công cơ bản

B.2.1. Tổng quan

Nhiều trường hợp thử nghiệm trong tiêu chuẩn này yêu cầu đánh giá xem liệu sức mạnh của một cơ chế an toàn từ Thiết bị camera có đủ hay không. Để tạo điều kiện cho việc đánh giá, các thuộc tính liên quan của một kẻ tấn công ở mức cơ bản được mô tả trong điều khoản này.

Nhìn chung, tiêu chuẩn này hướng tới một mức độ an toàn cơ bản. Nó nhằm mục đích đóng góp vào việc bảo vệ các thiết bị camera trước các mối đe dọa an toàn mạng phổ biến nhất, đặc biệt là qua các giao diện mạng. Các cuộc tấn công đa phương tiện hoặc nhắm mục tiêu/phức tạp cao không nằm trong phạm vi của tiêu chuẩn này. Mô hình kẻ tấn công được đặc trưng bởi sự kết hợp giữa khả năng và động cơ của kẻ tấn công.

B.2.2. Động cơ của kẻ tấn công

Mục tiêu của quy chuẩn này là một thiết bị tuân thủ được bảo vệ chống lại các cuộc tấn công cơ bản vào các điểm yếu thiết kế cơ bản, đặc biệt là liên quan đến các cuộc tấn công qua mạng. Một kịch bản tấn công điển hình là khi kẻ tấn công có ý định xâm nhập vào một loại thiết bị để tích hợp vào một mạng botnet nhằm tấn công bên thứ ba. Kẻ tấn công không có ý định xâm nhập vào thiết bị camera cụ thể. Nếu kẻ tấn công phát hiện rằng thiết bị camera không có những lỗ hổng cơ bản, hắn sẽ thường chuyển sang một thiết bị khác. Do đó, động cơ của kẻ tấn công là cơ bản để xâm nhập vào thiết bị camera.

B.2.3. Đặc trưng của kẻ tấn công

Khả năng của kẻ tấn công được đặc trưng bởi chuyên môn và tài nguyên. Nó được định lượng là tiềm năng tấn công, được xác định bởi các yếu tố sau đây được mô tả trong Bảng B.1.

Bảng B.1 - Đặc trưng của kẻ tấn công

Yếu tố	Mô tả	Tiềm năng của kẻ tấn công cơ bản
Thời gian trôi qua để xác định và khai thác	Thời gian trôi qua là tổng thời gian mà một kẻ tấn công mất để xác định rằng một lỗ hổng tiềm năng cụ thể tồn tại trong thiết bị camera, phát triển phương pháp tấn công và duy trì nỗ lực cần thiết để thực hiện cuộc tấn công vào thiết bị camera.	Thời gian trôi qua bị giới hạn dưới một tháng.
Chuyên môn	Chuyên môn đề cập đến mức độ kiến thức chung về các nguyên tắc cơ bản, loại sản phẩm hoặc các phương pháp tấn công.	Mức độ chuyên môn bị giới hạn ở một người thông thạo, người có quen thuộc với hành vi an toàn của loại sản phẩm này.
Kiến thức về thiết bị camera (thiết kế và vận hành)	Kiến thức về thiết bị camera đề cập đến kiến thức chuyên môn cụ thể liên quan đến thiết bị camera. Điều này khác với kiến thức chuyên môn chung, nhưng không phải là không liên quan.	Kiến thức về thiết bị camera bị giới hạn trong thông tin công khai liên quan đến thiết bị camera và thông tin cung cấp cho người sử dụng, ví dụ hướng dẫn sử dụng. Kiến thức được kiểm soát trong tổ chức phát triển và chia sẻ với các tổ chức khác dưới một thỏa thuận bảo mật không được bao gồm.
Cơ hội	Cơ hội có mối quan hệ với yếu tố thời gian trôi qua. Việc xác định hoặc khai thác một lỗ hổng có thể yêu cầu một lượng đáng kể quyền truy cập vào thiết bị camera, điều này có thể tăng khả năng bị phát hiện. Một số phương pháp tấn công có thể yêu cầu nỗ lực đáng kể ngoại tuyến, và chỉ cần quyền truy cập ngắn vào thiết bị camera để khai thác. Quyền truy cập cũng có thể cần liên tục hoặc qua nhiều phiên.	Cơ hội bị giới hạn ở mức độ vừa phải, tức là quyền truy cập vào thiết bị camera yêu cầu ít hơn một tháng và số lượng mẫu thiết bị camera cần thiết để thực hiện cuộc tấn công ít hơn một trăm.

Thiết bị cần thiết để khai thác	Thiết bị cần thiết để khai thác đề cập đến việc kẻ tấn công thu nhận thiết bị.	Thiết bị chuyên dụng không dễ dàng có sẵn cho kẻ tấn công, nhưng thu nhận được mà không cần nỗ lực quá mức và/hoặc với chi phí hợp lý, tạo thành giới hạn cao nhất về việc thu nhận thiết bị. Điều này bao gồm việc mua một lượng vừa phải thiết bị, hoặc phát triển các tập lệnh hoặc chương trình tấn công rộng rãi hơn.

B.3. Mô hình cho "người sử dụng có kiến thức kỹ thuật hạn chế"

B.3.1. Tổng quan

Nhiều trường hợp thử nghiệm trong tiêu chuẩn này yêu cầu đánh giá xem liệu tính khả dụng của một cơ chế liên quan đến an toàn từ thiết bị camera có được đảm bảo hay không và liệu các tài liệu hướng dẫn có dễ hiểu đối với người sử dụng phổ thông hay không. Để hỗ trợ quá trình đánh giá, các đặc điểm liên quan của một người sử dụng tương ứng được mô tả trong mục này.

B.3.2. Đặc trưng của "người sử dụng có kiến thức kỹ thuật hạn chế"

Bảng B.2 dưới đây mô tả các giả định về khả năng của một người sử dụng có kiến thức kỹ thuật hạn chế.

Bảng B.2 - Đặc trưng người sử dụng

Yếu tố	Mô tả	Tiềm năng của người sử dụng
Chuyên môn	Chuyên môn liên quan đến mức độ kiến thức chung về các nguyên tắc cơ bản và loại sản phẩm.	Mức độ chuyên môn được giới hạn ở mức cơ bản được mô tả bởi các dữ liệu chính sau: - Người sử dụng có khả năng sử dụng trình duyệt trang thông tin điện tử. - Người sử dụng có thể điều hướng qua Internet công cộng và điền vào các biểu mẫu. - Người sử dụng biết cách thay đổi cài đặt trong hệ điều hành điện thoại thông minh. - Người sử dụng có kiến thức cơ bản về an toàn (ví dụ: biết cách sử dụng máy quét virus hoặc mật khẩu, chẳng hạn như mật khẩu mạng không dây). - Người sử dụng có kiến thức cơ bản về các bản cập nhật an toàn (ví dụ: biết mục đích, biết rằng các bản cập nhật cần phải được truyền/tải và biết ý nghĩa của thời gian hỗ trợ). - Người sử dụng có khả năng ghép nối các thiết bị (ví dụ: tai nghe không dây với điện thoại thông minh). - Người sử dụng thường biết máy ảnh hoặc míc nói là gì.

Kiến thức về thiết bị camera	Kiến thức về thiết bị camera liên quan đến chuyên môn cụ thể đối với thiết bị camera. Điều này khác biệt với kiến thức chung nhưng không phải là không liên quan.	Kiến thức về thiết bị camera chỉ giới hạn trong tất cả thông tin được cung cấp hoặc tham khảo cùng với thiết bị camera (ví dụ: hướng dẫn sử dụng) và những gì công khai trên trang trang thông tin điện tử của nhà cung cấp. Người sử dụng biết chức năng dự kiến của thiết bị camera.
Thiết bị sử dụng thiết bị camera	Thiết bị cần thiết để sử dụng thiết bị camera.	Thiết bị của người sử dụng giới hạn ở những gì được cung cấp cùng với thiết bị camera (ví dụ: phần mềm bổ sung). Ngoài ra, người dùng còn sử dụng máy tính hoặc điện thoại thông minh hoặc các cổng kết nối và trung tâm kết nối nếu cần thiết.

Phụ lục C

(Quy định)

Mã HS thiết bị camera giám sát sử dụng giao thức Internet

TT	Tên sản phẩm, hàng hóa theo QCVN	Mã số HS	Mô tả sản phẩm, hàng hóa
01	Thiết bị camera giám sát sử dụng giao thức Internet	8525.83.10 8525.83.90 8525.89.10 8525.89.90	Camera kỹ thuật số, có thể kết nối qua giao thức Internet, thực hiện một phần hoặc toàn bộ việc giám sát, ghi hình.

Thư mục tài liệu tham khảo

[1] ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".

[2] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".

[3] ETSI TR 103 621 (V0.1.6) (2021-06): "CYBER; Guide to Cyber Security for Consumer Internet of Things".

[4] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[5] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[6] ISO/IEC 15408: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security".