BỘ CÔNG AN	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 48 /2026/TT-BCA	*Hà Nội, ngày 12 tháng 5 năm 2026*

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 ninh mạng cơ bản

Căn cứ Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật số 70/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Nghị định số 22/2026/NĐ-CP ngày 16 tháng 01 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức, hướng dẫn thi hành Luật Tiêu chuẩn và quy chuẩn kỹ thuật;

Căn cứ Nghị định số 02/2025/NĐ-CP ngày 18 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an được sửa đổi, bổ sung bởi Nghị định số 11/2025/NĐ-CP ngày 01 tháng 07 năm 2025 của Chính phủ;

Theo đề nghị của Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao;

Bộ trưởng Bộ Công an ban hành 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 ninh mạng 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 cầu an ninh mạng cơ bản - QCVN 11:2026/BCA.

Điều 2. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 07 năm 2026.

2. Thông tư số 21/2024/TT-BTTTT ngày 31 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông 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 (QCVN 135:2024/BTTTT) hết hiệu lực kể từ ngày Thông tư này có hiệu lực thi hành.

3. Việc công bố hợp quy đối với sản phẩm, hàng hóa quy định tại QCVN 11:2026/BCA được áp dụng khi Bộ Công an ban hành Danh mục sản phẩm, hàng hóa có mức độ rủi ro trung bình và mức độ rủi ro cao thuộc trách nhiệm quản lý.

Điều 3. Điều khoản thi hành

1. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao có trách nhiệm theo dõi, kiểm tra, đôn đốc việc thực hiện Thông tư này.

2. Cục Khoa học, chiến lược và lịch sử Công an chịu trách nhiệm tổ chức phổ biến Quy chuẩn này cho cơ quan, tổ chức, cá nhân có liên quan và chỉ định các tổ chức đánh giá sự phù hợp với Quy chuẩn này theo quy định của pháp luật.

3. Cục Khoa học, chiến lược và lịch sử Công an có trách nhiệm định kỳ cập nhật, chia sẻ danh sách các tổ chức, cá nhân và thiết bị camera đã hoàn thành công bố hợp quy cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao và Công an các đơn vị, địa phương có liên quan để phục vụ công tác quản lý theo quy định.

4. Thủ trưởng các đơn vị thuộc cơ quan Bộ, Giám đốc Công an tỉnh, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

Trong quá trình thực hiện Thông tư, nếu có khó khăn, vướng mắc, Công an các đơn vị, địa phương, tổ chức, cá nhân có liên quan báo cáo về Bộ Công an (qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để kịp thời hướng dẫn./.

Nơi nhận:
- Các đồng chí Thứ trưởng Bộ Công an;
- Văn phòng Chính phủ;
- Các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố;
- Cục Kiểm tra văn bản và Tổ chức thi hành pháp luật Bộ Tư pháp;
- Các đơn vị thuộc cơ quan Bộ Công an;
- Công an các tỉnh, thành phố;
- Công báo;
- Cổng TTĐT Chính phủ;
- Cổng TTĐT Bộ Công an;
- Lưu: VT, A05.

BỘ TRƯỞNG

Đại tướng Lương Tam Quang

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 11:2026/BCA

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ THIẾT BỊ CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET - CÁC YÊU CẦU AN NINH MẠNG CƠ BẢN

National technical regulation for Surveillance Camera using Internet Protocol - Baseline cybersecurity requirements

HÀ NỘI - 2026

Lời nói đầu

QCVN 11:2026/BCA do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Cục Khoa học, chiến lược và lịch sử Công an trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Công an ban hành theo Thông tư số /2026/TT-BCA ngày tháng năm 2026.

Mục lục

Lời nói đầu....3
1. QUY ĐỊNH CHUNG....8
1.1. Phạm vi điều chỉnh....8
1.2. Đối tượng áp dụng....8
1.3. Tài liệu viện dẫn....8
1.4. Chữ viết tắt....8
1.5. Giải thích từ ngữ....8
2. QUY ĐỊNH KỸ THUẬT....13
2.1. Khởi tạo mật khẩu duy nhất....13
2.1.1. Yêu cầu 2.1.1....13
2.1.2. Yêu cầu 2.1.2....13
2.1.3. Yêu cầu 2.1.3....13
2.1.4. Yêu cầu 2.1.4....13
2.1.5. Yêu cầu 2.1.5....13
2.2. Quản lý lỗ hổng bảo mật....13
2.2.1. Yêu cầu 2.2.1....13
2.3. Quản lý cập nhật....14
2.3.1. Yêu cầu 2.3.1....14
2.3.2. Yêu cầu 2.3.2....14
2.3.3. Yêu cầu 2.3.3....14
2.3.4. Yêu cầu 2.3.4....14
2.3.5. Yêu cầu 2.3.5....14
2.3.6. Yêu cầu 2.3.6....14
2.3.7. Yêu cầu 2.3.7....14
2.4. Lưu trữ các tham số an toàn nhạy cảm....14
2.4.1. Yêu cầu 2.4.1....14
2.4.2. Yêu cầu 2.4.2....14
2.4.3. Yêu cầu 2.4.3....14
2.4.4. Yêu cầu 2.4.4....14
2.5. Quản lý kênh giao tiếp an toàn....15

2.5.1. Yêu cầu 2.5.1 15
2.5.2. Yêu cầu 2.5.2 15
2.5.3. Yêu cầu 2.5.3 15
2.5.4. Yêu cầu 2.5.4 15
2.6. Phòng chống tấn công thông qua các giao diện của thiết bị 15
2.6.1. Yêu cầu 2.6.1 15
2.6.2. Yêu cầu 2.6.2 15
2.6.3. Yêu cầu 2.6.3 15
2.7. Bảo vệ dữ liệu người sử dụng 15
2.7.1. Yêu cầu 2.7.1 15
2.7.2. Yêu cầu 2.7.2 15
2.8. Khả năng tự khôi phục lại hoạt động bình thường sau sự cố 15
2.8.1. Yêu cầu 2.8.1 15
2.8.2. Yêu cầu 2.8.2 16
2.8.3. Yêu cầu 2.8.3 16
2.9. Xóa dữ liệu trên thiết bị camera 16
2.9.1. Yêu cầu 2.9.1 16
2.10. Xác thực dữ liệu đầu vào 16
2.10.1. Yêu cầu 2.10.1 16
2.11. Bảo vệ dữ liệu trên thiết bị camera 16
2.11.1. Yêu cầu 2.11.1 16
2.11.2. Yêu cầu 2.11.2 16
2.11.3. Yêu cầu 2.11.3 16
2.11.4. Yêu cầu 2.11.4 16
2.11.5. Yêu cầu 2.11.5 16
3. PHƯƠNG PHÁP ĐO 16
3.1. Khởi tạo mật khẩu duy nhất 16
3.1.1. Nhóm kiểm thử yêu cầu 2.1.1 16
3.1.2. Nhóm kiểm thử yêu cầu 2.1.2 18
3.1.3. Nhóm kiểm thử yêu cầu 2.1.3 19
3.1.4. Nhóm kiểm thử yêu cầu 2.1.4 20
3.1.5. Nhóm kiểm thử yêu cầu 2.1.5 21

3.2. Quản lý lỗ hổng bảo mật....22
3.2.1. Nhóm kiểm thử yêu cầu 2.2.1....22
3.3. Quản lý cập nhật....23
3.3.1. Nhóm kiểm thử yêu cầu 2.3.1....23
3.3.2. Nhóm kiểm thử yêu cầu 2.3.2....24
3.3.3. Nhóm kiểm thử yêu cầu 2.3.3....25
3.3.4. Nhóm kiểm thử yêu cầu 2.3.4....26
3.3.5. Nhóm kiểm thử yêu cầu 2.3.5....26
3.3.6. Nhóm kiểm thử yêu cầu 2.3.6....28
3.3.7. Nhóm kiểm thử yêu cầu 2.3.7....28
3.4. Lưu trữ các tham số an toàn nhạy cảm....29
3.4.1. Nhóm kiểm thử yêu cầu 2.4.1....29
3.4.2. Nhóm kiểm thử yêu cầu 2.4.2....31
3.4.3. Nhóm kiểm thử yêu cầu 2.4.3....32
3.4.4. Nhóm kiểm thử yêu cầu 2.4.4....33
3.5. Quản lý kênh giao tiếp an toàn....34
3.5.1. Nhóm kiểm thử yêu cầu 2.5.1....34
3.5.2. Nhóm kiểm thử yêu cầu 2.5.2....35
3.5.3. Nhóm kiểm thử yêu cầu 2.5.3....37
3.5.4. Nhóm kiểm thử yêu cầu 2.5.4....38
3.6. Phòng chống tấn công thông qua các giao diện của thiết bị....39
3.6.1. Nhóm kiểm thử yêu cầu 2.6.1....39
3.6.2. Nhóm kiểm thử yêu cầu 2.6.2....40
3.6.3. Nhóm kiểm thử yêu cầu 2.6.3....41
3.7. Bảo vệ dữ liệu người sử dụng....42
3.7.1. Nhóm kiểm thử yêu cầu 2.7.1....42
3.7.2. Nhóm kiểm thử yêu cầu 2.7.2....44
3.8. Khả năng tự khôi phục lại hệ thống bình thường sau sự cố....44
3.8.1. Nhóm kiểm thử yêu cầu 2.8.1....44
3.8.2. Nhóm kiểm thử yêu cầu 2.8.2....45
3.8.3. Nhóm kiểm thử yêu cầu 2.8.3....47

3.9. Xoá dữ liệu trên thiết bị camera.....47
3.9.1. Nhóm kiểm thử yêu cầu 2.9.1 47
3.10. Xác thực dữ liệu đầu vào.....49
3.10.1. Nhóm kiểm thử yêu cầu 2.10.1.....49
3.11. Bảo vệ dữ liệu trên thiết bị camera.....50
3.11.1. Nhóm kiểm thử yêu cầu 2.11.1.....50
3.11.2. Nhóm kiểm thử yêu cầu 2.11.2.....51
3.11.3. Nhóm kiểm thử yêu cầu 2.11.3.....52
3.11.4. Nhóm kiểm thử yêu cầu 2.11.4.....53
3.11.5. Nhóm kiểm thử yêu cầu 2.11.5.....54
4. QUY ĐỊNH VỀ QUẢN LÝ.....56
Phụ lục A Danh mục thông tin phục vụ đánh giá.....57

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ THIẾT BỊ CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET - CÁC YÊU CẦU AN NINH MẠNG 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 ninh mạng cơ bản cho thiết bị camera giám sát sử dụng giao thức Internet (Sau đây gọi tắt là thiết bị camera) được sản xuất, lưu hành tại thị trường Việt Nam.

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) các thiết bị camera 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

1.5. Giải thích từ ngữ

Trong 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 thiết bị camera sử dụng để xác thực truy cập, sử dụng các tính năng.

1.5.3. Giá trị xác thực (Authentication value)

Thông tin được sử dụng để xác thực theo 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 khả năng khai thác lỗ hổng bảo mật với các kỹ thuật hiện có.

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.

1.5.5. Khoảng thời gian hỗ trợ (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.

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 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.

1.5.12. 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.

1.5.13. 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.

1.5.14. 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 sản phẩm hoặc để thực hiện phân tích vấn đề của thiết bị và người sử dụng không được sử dụng giao diện này.

1.5.15. Giao diện logic (Logical interface)

Giao diện để giao tiếp với thiết bị thông qua các kênh hoặc cổng kết nối với thiết bị.

1.5.16. 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.

1.5.17. Giao diện vật lý (Physical interface)

Giao diện được sử dụng để kết nối với thiết bị thông qua cổng vật lý hoặc giao diện kết nối vô tuyến.

Ví dụ: Cổng Ethernet; Cổng USB; Wifi.

1.5.18. Mật khẩu khởi tạo (Initial password)

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

1.5.19. Mật khẩu mặc định (Default password)

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

1.5.20. Khởi tạo (Initialization)

Quá trình kích hoạt 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.

1.5.21. 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.

1.5.22. 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 của một mô-đun an toàn.

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

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

Tham số an toàn bao gồm là tham số an toàn quan trọng và tham số an toàn công khai.

1.5.24. Mô-đun an toàn (Security module)

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

1.5.25. Cập nhật an toàn (Security update)

Hoạt động do nhà sản xuất thực hiện để cập nhật phần mềm nhằm xử lý các lỗ hổng bảo mật của thiết bị.

1.5.26. Dịch vụ phần mềm (Software service)

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

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

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

Trạng thái của thiết bị sau khi khởi tạo.

1.5.28. Truy cập từ xa (Remotely accessible)

Việc truy cập thiết bị camera từ bên ngoài mạng nội bộ.

1.5.29. 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.

1.5.30. 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.

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

Tập hợp thông tin trong hồ sơ kỹ thuật dùng để mô tả hoặc tham chiếu các dữ liệu bổ sung (ngoài các thông tin đã được cung cấp trong ICS) liên quan đến thiết bị camera và môi trường đánh giá, giúp phòng đo kiểm thực hiện các hoạt động kiểm thử tuân thủ.

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

Tài liệu dưới dạng bảng câu hỏi do nhà sản xuất cung cấp được sử dụng để hỗ trợ xây dựng thông tin triển khai bổ sung cho kiểm thử đối với thiết bị camera.

1.5.33. 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.

1.5.34. Cam kết an toàn (Security guarantee)

Tuyên bố về các mục tiêu an toàn do nhà sản xuất triển khai, thực hiện.

CHÚ THÍCH: Trong Quy 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 vận hành cụ thể.

1.5.35. 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.

1.5.36. 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.

1.5.37. 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.

1.5.38. 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.

1.5.39. Bằng chứng bên ngoài (External evidence)

Các chứng nhận an toàn hiện có hoặc kết quả đánh giá của bên thứ ba về một phần hoặc toàn bộ 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.

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

Hoạt động đánh giá nhằm xác định mức độ tuân thủ của tài liệu IXIT đối với các yêu cầu quy định tại Quy chuẩn này.

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

Hoạt động đánh giá nhằm xác định mức độ tuân thủ của các chức năng được triển khai trên thiết bị camera, bao gồm mối quan hệ giữa các chức năng này với các dịch vụ liên quan và/hoặc các quy trình phát triển, quản lý theo yêu cầu của quy định tại Quy chuẩn này, phục vụ cho việc chứng minh sự tuân thủ về triển khai.

1.5.42. Thiết bị camera giám sát sử dụng giao thức Internet (Surveillance Camera using Internet Protocol)

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.

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.

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 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 bao gồm tối thiểu các thông tin sau:

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

2) Thông tin về thời gian đối với việc:

2.1) Xác nhận ban đầu về việc nhận được báo cáo;

2.2) 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 thông báo cho người sử dụng khi các phần mềm có bản cập nhật và hỗ trợ cập nhật, cài đặt các phần mềm một cách an toàn.

2.3.2. Yêu cầu 2.3.2

Thiết bị camera có cơ chế cho phép người sử dụng cập nhật phần mềm.

2.3.3. Yêu cầu 2.3.3

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

2.3.4. Yêu cầu 2.3.4

Nhà sản xuất có chính sách, quy trình triển khai việc cung cấp bản cập nhật an toàn.

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 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 thông tin định danh duy nhất được cứng hóa trên thiết bị camera dùng trong mục đích bảo mật, 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 cứng hóa trong mã nguồn của thiết bị camera phải có biện pháp bảo vệ và mục đích sử dụng phù hợp.

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 là duy nhất cho mỗi thiết bị và 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 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 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 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 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 thiết bị camera có giao diện gỡ lỗi có thể truy cập được ở mức vật lý thì 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 được bảo vệ bằng cách ứng dụng các mật mã an toàn 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 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 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 khôi phục được hoạt động sau khi bị mất kết nối mạng và mất điện.

2.8.3. Yêu cầu 2.8.3

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

2.9. Xóa dữ liệu trên thiết bị camera

2.9.1. 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

Thiết bị camera xác thực dữ liệu đầu vào từ giao diện người sử dụng hoặc dữ liệu đầu vào được truyền qua các giao diện lập trình ứng dụng 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 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 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 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 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

3.1.1.2.1. Mục đích kiểm thử

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

3.1.1.2.2. Phương pháp kiểm thử

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.

3.1.1.2.3. Kết luận

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

1.1) 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.

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

3.1.1.3. Đánh giá sự tuân thủ về triển khai

3.1.1.3.1. 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 (Mục 1 tại 3.1.1.3.2), các mật khẩu do người sử dụng định nghĩa (Mục 2 tại 3.1.1.3.2) và các cơ chế khởi tạo mật khẩu (Mục 3 tại 3.1.1.3.2).

3.1.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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".

3.1.1.3.3. Kết luận

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

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

1.2) 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.

1.3) 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.

2) 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

3.1.2.2.1. 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.

3.1.2.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

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

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

3.1.2.2.3. Kết luận

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

1.1) Không có quy tắc rõ ràng trong các mật khẩu được cài đặt sẵn;

1.2) Không tìm thấy các chuỗi thông dụng hoặc có quy luật thông dụng trong các mật khẩu được cài đặt sẵn;

1.3) Các cơ chế khởi tạo mật khẩu không tạo các mật khẩu được cài đặt sẵn có liên quan đến thông tin công khai;

1.4) Các cơ chế khởi tạo mật khẩu tạo các mật khẩu được cài đặt sẵn đáp ứng các yêu cầu về độ phức tạp.

2) 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

3.1.2.3.1. 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.

3.1.2.3.2. Phương pháp kiểm thử

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.

3.1.2.3.3. Kết luận

1) Đáp ứng: 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.

2) 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.

Mục tiêu của nhóm kiểm thử này là để xác nhận rằng các phương thức mã hóa của thiết bị camera có khả năng ngăn chặn tấn công bằng các kỹ thuật hiện có.

3.1.3.2. Đánh giá sự tuân thủ về thiết kế

3.1.3.2.1. 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 (Mục 1, 2, 3 tại 3.1.3.2.2) và hạn chế khả năng bị bẻ khoá (Mục 4 tại 3.1.3.2.2).

3.1.3.2.2. Phương pháp kiểm thử

1) 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.

2) 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 cơ chế xác thực được mô tả trong "Mô tả" có đảm bảo được các "Cam kết an toàn" hay không.

3) 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.

4) 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" hạn chế khả năng bị bẻ khoá bằng các kỹ thuật hiện có 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.

3.1.3.2.3. Kết luận

1) 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:

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

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

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

1.4) Tất cả các "Phương thức mã hóa" không được biết là hạn chế khả năng khai thác với các thuộc tính an toàn.

2) 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

3.1.3.3.1. 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.

3.1.3.3.2. 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.

3.1.3.3.3. Kết luận

1) Đáp ứng: Bất kỳ phương thức mã hoá được sử dụng phải tuân thủ theo mô tả trong IXIT.

2) 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

3.1.4.2.1. Mục đích kiểm thử

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

3.1.4.2.2. Phương pháp kiểm thử

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 cách thức thay đổi giá trị xác thực cho người sử dụng có kiến thức kỹ thuật hạn chế.

3.1.4.2.3. Kết luận

1) Đáp ứng: 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.

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

3.1.4.3. Đánh giá sự tuân thủ về triển khai

3.1.4.3.1. Mục đích kiểm thử

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

3.1.4.3.2. Phương pháp kiểm thử

1) Phòng đo kiểm thực hiện thay đổi các giá trị xác thực theo 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.

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

3.1.4.3.3. Kết luận

1) Đáp ứng: Tất cả các cơ chế xác thực cho phép người sử dụng thay đổi giá trị xác thực hoạt động đúng như mô tả.

2) 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

3.1.5.2.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế cơ chế xác thực của thiết bị camera khiến không thể thực hiện tấn công vét cạn thông qua giao diện mạng.

3.1.5.2.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá đối với mỗi cơ chế xác thực trong IXIT 1-AuthMech với phần "Mô tả" cho thấy cơ chế xác thực có thể truy cập trực tiếp qua giao diện mạng, cơ chế xác thực trong "Ngăn chặn tấn công vét cạn" có khả năng vô hiệu hóa việc tấn công vét cạn thông qua giao diện mạng.

3.1.5.2.3. Kết luận

1) Đáp ứng: Cơ chế xác thực được tài liệu hoá đảm bảo khả năng vô hiệu hóa tấn công vét cạn thông qua giao diện mạng.

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

3.1.5.3. Đánh giá sự tuân thủ về triển khai

3.1.5.3.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với việc cơ chế vô hiệu hóa việc tấn công vét cạn thông qua giao diện mạng, bao gồm tính đầy đủ của tài liệu IXIT (Mục 1 tại 3.1.5.3.2) và các cơ chế tương ứng (Mục 2 tại 3.1.5.3.2).

3.1.5.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.1.5.3.3. Kết luận

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

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

1.2) 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.

2) 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

3.2.1.2.1. 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.

3.2.1.2.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá việc truy cập vào chính sách công bố thông tin về lỗ hổng bảo mật 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 và là liệu bất kỳ ai cũng truy cập vào được hay không.

3.2.1.2.3. Kết luận

1) Đáp ứng: Chính sách công bố lỗ hổng bảo mật được công khai.

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

3.2.1.3. Đánh giá sự tuân thủ về triển khai

3.2.1.3.1. 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.

3.2.1.3.2. Phương pháp kiểm thử

1) 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.

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

2.1) Thông tin liên hệ;

2.2) Thông tin về thời gian liên quan đến việc tiếp nhận thông tin và cập nhật trạng thái.

3.2.1.3.3. Kết luận

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

1.2) Chính sách công bố lỗ hổng bảo mật được công khai;

1.3) 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.

2) 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 thông báo cho người sử dụng khi các phần mềm có bản cập nhật và 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

3.3.1.2.1. 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.

3.3.1.2.2. 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.

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.

3.3.1.2.3. Kết luận

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

1.1) Có cơ chế thông báo cho người sử dụng khi các phần mềm có bản cập nhật.

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

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

3.3.1.3. Đánh giá sự tuân thủ về triển khai

3.3.1.3.1. 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.

3.3.1.3.2. Phương pháp kiểm thử

1) 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".

2) 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".

3.3.1.3.3. Kết luận

1) Đáp ứng: Không có khả năng lợi dụng một cơ chế cập nhật trên thiết bị camera.

2) 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.

Trong nhóm kiểm thử này, một bản cập nhật để triển khai áp dụng bao gồm việc áp dụng tự động hoặc được khởi tạo bằng cách sử dụng một dịch vụ liên quan (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 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

3.3.2.2.1. 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.

3.3.2.2.2. Phương pháp kiểm thử

1) 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:

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

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

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

1.4) Bản cập nhật phần mềm sử dụng phương thức tương tự phù hợp với người sử dụng có kiến thức kỹ thuật hạn chế.

3.3.2.2.3. Kết luận

1) Đáp ứng: Mỗi thành phần phần mềm hỗ trợ ít nhất một cơ chế cập nhật đơn giản để người sử dụng áp dụng.

2) 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.

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

3.3.3.2.1. 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 (Mục 1, 2, 3 tại 3.3.3.2.2) và hạn chế khả năng bị bẻ khoá (Mục 4 tại 3.3.3.2.2).

3.3.3.2.2. Phương pháp kiểm thử

1) 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 tính xác thực.

2) 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.

3) 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.

4) Đối với mỗi cơ chế cập nhật trong IXIT 7-UpdMech, Phòng đo kiểm đánh giá "Phương thức mã hóa" hạn chế khả năng bị bẻ khoá bằng các kỹ thuật hiện có 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.

3.3.3.2.3. Kết luận

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

1.1) Các Cam kết an toàn đáp ứng trong các trường hợp cập nhật an toàn;

1.2) Cơ chế cập nhật đáp ứng được các Cam kết an toàn đối với các trường hợp sử dụng;

1.3) Tất cả các "Phương thức mã hóa" được sử dụng coi là Mật mã an toàn đối với trường hợp sử dụng;

1.4) Tất cả các "Phương thức mã hóa" không được biết là hạn chế khả năng bị bẻ khoá với các thuộc tính an toàn.

2) 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.

3.3.4.2. Đánh giá sự tuân thủ về thiết kế

3.3.4.2.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với cách thức triển khai các bản cập nhật an toàn (Mục 1 tại 3.3.4.2.2) và xác nhận rằng các điều kiện tiên quyết cho việc triển khai đã được đảm bảo (Mục 2 tại 3.3.4.2.2).

3.3.4.2.2. Phương pháp kiểm thử

1) 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.

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

3.3.4.2.3. Kết luận

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

1.1) Quy trình quản lý cập nhật đáp ứng yêu cầu về cập nhật an toàn;

1.2) Có xác nhận về việc triển khai.

2) 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.

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

3.3.5.2.1. 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 (Mục 1 tại 3.3.5.2.2) và đối tượng thực hiện (Mục 2 tại 3.3.5.2.2), cùng với việc đánh giá sự tuân thủ về triển khai đối với tính đầy đủ của tài liệu IXIT.

3.3.5.2.2. Phương pháp kiểm thử

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

1.1) 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, 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.

1.2) 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.

2) 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:

2.1) Kênh truyền được xác thực;

2.2) Thiết bị camera tham gia một mạng lưới yêu cầu sở hữu một tham số bảo mật quan trọng hoặc mật khẩu để tham gia;

2.3) Xác minh bằng chữ ký số của bản cập nhật;

2.4) Xác nhận bởi người sử dụng;

2.5) Một chức năng bảo mật tương đương.

3) 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.

3.3.5.2.3. Kết luận

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

1.1) 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;

1.2) 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;

1.3) 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;

1.4) Mọi cơ chế cập nhật dựa trên giao diện mạng được phát hiện đều được mô tả trong IXIT.

2) 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.

3.3.6.2. Đánh giá sự tuân thủ về thiết kế

3.3.6.2.1. Mục đích kiểm thử

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

3.3.6.2.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá việc truy cập thông tin về "Công bố thời gian hỗ trợ" trong IXIT 2-UserInfo có đảm bảo rõ ràng đối với người sử dụng có kiến thức kỹ thuật hạn chế.

3.3.6.2.3. Kết luận

1) Đáp ứng: Việc công bố thời gian hỗ trợ cập nhật phần mềm đảm bảo rõ ràng đối với người sử dụng có kiến thức kỹ thuật hạn chế.

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

3.3.6.3. Đánh giá sự tuân thủ về triển khai

3.3.6.3.1. Mục đích kiểm thử

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

3.3.6.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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.

3.3.6.3.3. Kết luận

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

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

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

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

2) 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

3.3.7.2.1. Mục đích kiểm thử

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

3.3.7.2.2. Phương pháp kiểm thử

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.

3.3.7.2.3. Kết luận

1) Đáp ứng: 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.

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

3.3.7.3. Đánh giá sự tuân thủ về triển khai

3.3.7.3.1. Mục đích kiểm thử

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

3.3.7.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.3.7.3.3. Kết luận

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

1.1) Model thiết bị camera có thể được trích xuất theo cách nhận dạng được mô tả;

1.2) Model thiết bị có sẵn dưới dạng văn bản đơn giản;

1.3) Model thiết bị khớp với Model thiết bị trong IXIT.

2) 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.

3.4.1.2. Đánh giá sự tuân thủ về thiết kế

3.4.1.2.1. 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 và tính đầy đủ của tài liệu IXIT.

3.4.1.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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.

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:

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

3.2) 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;

3.3) 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.

4) 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.

3.4.1.2.3. Kết luận

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

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

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

1.3) Mỗi tham số an toàn nhạy cảm có cơ chế bảo vệ phù hợp đối với các Cam kết an toàn được áp dụng;

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

2) 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

3.4.1.3.1. 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.

3.4.1.3.2. Phương pháp kiểm thử

1) 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.

3.4.1.3.3. Kết luận

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

2) 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 cứng hóa trên mỗi thiết bị là một giá trị riêng biệt và tĩnh, đại diện cho thiết bị và các thông tin tiềm ẩn được cứng hóa mà giá trị dẫn xuất từ đó.

Nhóm kiểm thử này liên quan đến việc xác định các định danh được cứng hóa 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.

3.4.2.2. Đánh giá sự tuân thủ về thiết kế

3.4.2.2.1. Mục đích kiểm thử

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

3.4.2.2.2. Phương pháp kiểm thử

1) 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 đã được cứng hóa, có một tuyên bố rõ ràng tương ứng được cung cấp.

2) Phòng đo kiểm đánh giá liệu đối với mỗi định danh đã được cứng hóa 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.

3) Phòng đo kiểm đánh giá liệu "Biện pháp bảo vệ" của mỗi định danh đã được cứng hóa 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.

3.4.2.2.3. Kết luận

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

1.1) Bất kỳ định danh đã được cứng hóa nào đều được tài liệu hóa tương ứng;

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

1.3) Mỗi định danh đã được cứng hóa có một cơ chế bảo vệ cho khả năng chống giả mạo.

2) 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

3.4.2.3.1. Mục đích kiểm thử

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

3.4.2.3.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá đối với mỗi định danh đã được cứng hóa 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.

3.4.2.3.3. Kết luận

1) Đáp ứng: Đối với mọi định danh đã được cứng hóa, việc triển khai bất kỳ cơ chế bảo vệ nào liên quan đến khả năng chống giả mạo tuân thủ tài liệu IXIT.

2) 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.

Nhóm kiểm thử này đánh giá thiết bị camera có tham số an toàn quan trọng được cứng hóa trong mã nguồn phần mềm không được tài liệu hóa trong các cơ chế cung cấp tham số an toàn quan trọng hay không.

3.4.3.2. Đánh giá sự tuân thủ về thiết kế

3.4.3.2.1. Mục đích kiểm thử

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

3.4.3.2.2. Phương pháp kiểm thử

1) 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 cứng hóa trong mã nguồn phần mềm của thiết bị và được phản ánh trong "Mô tả" hay không.

2) Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng trong IXIT 10-SecParam, mà được cứng hóa 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.

3.4.3.2.3. Kết luận

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

1.1) Bất kỳ tham số an toàn quan trọng nào được cứng hóa trong mã nguồn phần mềm của thiết bị đều được tài liệu hóa;

1.2) Đối với tất cả các tham số an toàn quan trọng được cứng hóa 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.

2) 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

3.4.3.3.1. Mục đích kiểm thử

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

3.4.3.3.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá đối với tất cả các tham số an toàn quan trọng được cứng hóa 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.

3.4.3.3.3. Kết luận

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

2) 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

3.4.4.2.1. 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.

3.4.4.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.4.4.2.3. Kết luận

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

1.1) 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";

1.2) 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.

2) 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 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 liệu các phương pháp mã hóa có hạn chế khả năng bị bẻ khoá hay không.

3.5.1.2. Đánh giá sự tuân thủ về thiết kế

3.5.1.2.1. 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 ninh mạng được công bố bởi các cơ quan, tổ chức trong nước hoặc nước ngoài tại thời điểm đánh giá.

3.5.1.2.2. Phương pháp đánh giá

1) 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 kênh giao tiếp hay không.

2) 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.

3) 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.

4) Đối với mỗi cơ chế kết nối trong IXIT 11-ComMech, đánh giá liệu "phương thức mã hóa" không bị khai thác bằng các kỹ thuật hiện có 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.

3.5.1.2.3. Kết luận đánh giá

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

1.1) Các Cam kết an toàn phù hợp với trường hợp sử dụng giao tiếp an toàn;

1.2) Cơ chế kết nối phù hợp để đạt được các Cam kết an toàn liên quan đến trường hợp sử dụng;

1.3) Tất cả các "phương thức mã hóa" được sử dụng được coi là mật mã an toàn cho trường hợp sử dụng;

1.4) Tất cả các "phương thức mã hóa" được sử dụng được biết là hạn chế khả năng bị bẻ khoá đối với thuộc tính an toàn mong muốn.

2) 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

3.5.1.3.1. 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.

3.5.1.3.2. 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.

3.5.1.3.3. Kết luận đánh giá

1) 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.

2) 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

3.5.2.2.1. 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.

3.5.2.2.2. 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.

1) 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".

2) 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 hoặc các yếu tố xác thực không hợp lệ hay không.

3) 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.

4) 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.

3.5.2.2.3. Kết luận

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

1.1) 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;

1.2) 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 hoặc các yếu tố xác thực không hợp lệ;

1.3) 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;

1.4) Mọi cơ chế ủy quyền cho phép truy cập đối với các đối tượng đã xác thực với quyền truy cập hợp lệ;

1.5) 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.

2) 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

3.5.2.3.1. 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.

3.5.2.3.2. Phương pháp kiểm thử

1) 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.

1.1) 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.

1.2) 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.

1.3) 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.

2) 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.

3.5.2.3.3. Kết luận

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

1.1) 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;

1.2) Đối tượng đã được xác thực với quyền truy cập thích hợp truy cập chức năng của thiết bị;

1.3) Không có dấu hiệu nào cho thấy cơ chế bảo vệ xác thực khác với tài liệu IXIT;

1.4) Mọi cơ chế kết nối dựa trên mạng được phát hiện đều được tài liệu hóa trong IXIT.

2) 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 hạn chế khả năng bị bẻ khoá.

3.5.3.2. Đánh giá sự tuân thủ về thiết kế

3.5.3.2.1. 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.

3.5.3.2.2. Phương pháp kiểm thử

1) 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.

3.5.3.2.3. Kết luận

1) 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:

1.1) Cam kết an toàn đáp ứng trường hợp sử dụng giao tiếp an toàn;

1.2) Cơ chế phù hợp để đáp ứng Cam kết an toàn đối với trường hợp sử dụng;

1.3) Phương thức mã hóa được coi là mật mã an toàn đối với trường hợp sử dụng;

1.4) Phương thức mã hóa được biết là hạn chế khả năng bị tấn công, khai thác.

2) 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

3.5.3.3.1. 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.

3.5.3.3.2. Phương pháp kiểm thử

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.

3.5.3.3.3. Kết luận

1) Đáp ứng: Bất kỳ phương thức mã hoá nào được sử dụng tuân thủ tài liệu IXIT của nó.

2) 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

3.5.4.2.1. 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 (Mục 1 tại 3.5.4.2.2) và đảm bảo các điều kiện tiên quyết cho việc thực hiện (Mục 2 tại 3.5.4.2.2).

3.5.4.2.2. Phương pháp kiểm thử

1) 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:

1.1) Khởi tạo;

1.2) Cung cấp;

1.3) Lưu trữ;

1.4) Cập nhật;

1.5) Ngừng hoạt động, lưu trữ và hủy bỏ;

1.6) Các quy trình xử lý việc hết hạn và bị xâm phạm.

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

3.5.4.2.3. Kết luận

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

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

1.2) Có một sự xác nhận cho việc thực hiện.

2) 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 cần đảm bảo rằng việc truy cập đến một giao diện logic đều được xác định. Căn cứ mục đích sử dụng, nhà sản xuất vô hiệu hóa những giao diện mạng và logic không cần thiết để cung cấp chức năng của thiết bị.

3.6.1.2. Đánh giá sự tuân thủ về thiết kế

3.6.1.2.1. Mục đích kiểm thử

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

3.6.1.2.2. 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.

3.6.1.2.3. Kết luận

1) Đáp ứng: Đối với mỗi giao diện mạng hoặc logic được đánh dấu là hoạt động trong tài liệu IXIT, có một mục đích cho việc giao diện đó được kích hoạt.

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

3.6.1.3. Đánh giá sự tuân thủ về triển khai

3.6.1.3.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các giao diện mạng và logic của thiết bị camera (Mục 1 tại 3.6.1.3.2) và tính đầy đủ của tài liệu IXIT (Mục 2 tại 3.6.1.3.2).

3.6.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.6.1.3.3. Kết luận

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

1.1) 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;

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

2) 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 Wifi®, ARP, DNS.

3.6.2.2. Đánh giá sự tuân thủ về thiết kế

3.6.2.2.1. 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.

3.6.2.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.6.2.2.3. Kết luận

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

1.2) 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;

1.3) 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.

2) 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

3.6.2.3.1. 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.

3.6.2.3.2. Phương pháp kiểm thử

Đối với mỗi giao diện mạng trong IXIT 15-Intf, Phòng đo kiểm đánh giá tính an toàn của thiết bị camera từ việc truy cập thiết bị camera thông qua giao diện mạng và logic mà không cần xác thực trong trạng thái khởi tạo, thông tin thu thập được chỉ thuộc mô tả trong phần "Thông tin được phép tiết lộ".

3.6.2.3.3. Kết luận

1) Đáp ứng: 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.

2) 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, nếu giao diện gỡ lỗi 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. Việc sử dụng các công cụ để truy cập trực tiếp vào phần cứng không nằm trong phạm vi đánh giá.

3.6.3.2. Đánh giá sự tuân thủ về thiết kế

3.6.3.2.1. Mục đích kiểm thử

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

3.6.3.2.2. Phương pháp kiểm thử

1) Đối với mỗi giao diện gỡ lỗi trong IXIT 15-Intf được mô tả là giao diện gỡ lỗi có thể truy cập theo thông tin tại "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.

2) Đối với mỗi giao diện gỡ lỗi 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.

3) Đối với mỗi giao diện gỡ lỗi 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.

3.6.3.2.3. Kết luận

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

1.1) Đối với mọi giao diện gỡ lỗi có thể truy cập, có một phần mềm được mô tả để vô hiệu hóa giao diện;

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

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

2) 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

3.6.3.3.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về triển khai đối với các giao diện gỡ lỗi có thể truy cập của thiết bị camera (Mục 1 tại 3.6.3.3.2) và tính đầy đủ của tài liệu IXIT (Mục 2 tại 3.6.3.3.2).

3.6.3.3.2. Phương pháp kiểm thử

1) Đối với mỗi giao diện mạng 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.

2) Đối với mỗi giao diện mạng có thể truy cập trên thiết bị camera, phòng đo kiểm đánh giá liệu giao diện đó 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.

3.6.3.3.3. Kết luận

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

1.2) Mọi giao diện gỡ lỗi có thể truy cập đều bị vô hiệu hóa;

1.3) Mọi giao diện gỡ lỗi đều được tài liệu hoá trong tài liệu IXIT.

2) 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 tính an toàn ở mức tối thiểu.

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

3.7.1.2. Đánh giá sự tuân thủ về thiết kế

3.7.1.2.1. 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.

3.7.1.2.2. 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 về tính bảo mật.

3.7.1.2.3. Kết luận

1) 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:

1.1) 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;

1.2) Cơ chế đáp ứng được các Cam kết an toàn đối với trường hợp sử dụng;

1.3) Tất cả phương pháp mã hóa được sử dụng coi là Mật mã an toàn đối với trường hợp sử dụng;

1.4) Tất cả phương pháp mã hóa được sử dụng không có khả năng bị tấn công.

2) 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

3.7.1.3.1. 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.

3.7.1.3.2. 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.

3.7.1.3.3. Kết luận

1) Đáp ứng: Bất kỳ phương thức mã hóa được sử dụng tuân thủ tài liệu IXIT tương ứng.

2) 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 khả năng 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.

3.7.2.2. Đánh giá sự tuân thủ về triển khai

3.7.2.2.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế đối với các khả năng cảm biến bên ngoài (Mục 1, 2 tại 3.7.2.2.2) và tính đầy đủ của tài liệu IXIT (Mục 3 tại 3.7.2.2.2).

3.7.2.2.2. Phương pháp kiểm thử

1) Phòng đo kiểm đánh giá việc về các khả năng cảm biến của thiết bị camera được sử dụng như thông tin trong phần "Tài liệu mô tả về các cảm biến thiết bị camera sử dụng" trong IXIT 2-UserInfo.

2) 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 đảm bảo rõ ràng đối với người sử dụng có kiến thức kỹ thuật hạn chế hay không.

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

3.7.2.2.3. Kết luận

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

1.1) Tài liệu truy cập được theo như mô tả trong IXIT;

1.2) Tài liệu đảm bảo rõ ràng đối với người sử dụng có kiến thức kỹ thuật hạn chế;

1.3) Mỗi khả năng cảm biến của thiết bị camera đều được tài liệu hoá cho người sử dụng.

2) 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

3.8.1.2.1. 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.

3.8.1.2.2. Phương pháp kiểm thử

1) 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".

2) 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".

3.8.1.2.3. Kết luận

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

1.1) Các cơ chế khôi phục đáp ứng để bảo vệ trước sự cố mạng và mất điện;

1.2) Mỗi cơ chế chống chịu đáp ứng được các Cam kết an toàn.

2) 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

3.8.1.3.1. 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.

3.8.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.8.1.3.3. Kết luận

1) Đáp ứng: 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.

2) 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

3.8.2.2.1. 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 (Mục 1 tại 3.8.2.2.2), các hoạt động trong quá trình mất kết nối mạng (Mục 2 tại 3.8.2.2.2) và quá trình khôi phục sau khi gặp sự cố về điện (Mục 3 tại 3.8.2.2.2).

3.8.2.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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.

3.8.2.2.3. Kết luận

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

1.1) Các cơ chế khôi phục đáp ứng việc bảo vệ trước sự cố kết nối mạng và điện;

1.2) Mỗi cơ chế khôi phục đáp ứng các Cam kết an toàn tương ứng;

1.3) 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;

1.4) Các cơ chế khôi phục đảm bảo thiết bị camera khôi phục hoàn toàn sau khi mất điện.

2) 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

3.8.2.3.1. 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.

3.8.2.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.8.2.3.3. Kết luận

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

1.1) 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;

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

1.3) 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.

2) 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.

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

1.1) Thực hiện thiết lập kết nối theo tiêu chuẩn;

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

3.8.3.2. Đánh giá sự tuân thủ về thiết kế

3.8.3.2.1. 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.

3.8.3.2.2. Phương pháp kiểm thử

1) 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.

2) 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.

3.8.3.2.3. Kết luận

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

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

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

2) 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

3.8.3.3.1. 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.

3.8.3.3.2. Phương pháp kiểm thử

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.

3.8.3.3.3. Kết luận

1) Đáp ứng: Hoạt động của bất kỳ biện pháp khôi phục nào đã triển khai tuân thủ tài liệu IXIT tương ứng.

2) 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

3.9.1.2.1. 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.

3.9.1.2.2. Phương pháp kiểm thử

1) 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 theo thông tin về "Mô tả" và "Khởi tạo và tương tác" để xóa dữ liệu khỏi thiết bị đối với từng "Loại đối tượng".

2) 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.

3) 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 và các giá trị mã hóa liên quan.

3.9.1.2.3. Kết luận

1) Đáp ứng: Thiết bị camera 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:

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

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

1.3) 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.

2) 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

3.9.1.3.1. 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.

3.9.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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.

3.9.1.3.3. Kết luận

1) 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:

1.1) Việc khởi tạo và tương tác của người sử dụng phù hợp với IXIT;

1.2) Dữ liệu người sử dụng được xóa thành công.

2) 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 quá trình xử lý dữ liệu mà không phát sinh 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.

3.10.1.2. Đánh giá sự tuân thủ về thiết kế

3.10.1.2.1. 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.

3.10.1.2.2. Phương pháp kiểm thử

1) 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:

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

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

1.3) 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.

2) 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.

3.10.1.2.3. Kết luận

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

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

1.2) 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.

2) 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

3.10.1.3.1. 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 (Mục 1 tại 3.10.1.3.2) và tính đầy đủ của tài liệu IXIT (Mục 2, 3 tại 3.10.1.3.2).

3.10.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

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

3.10.1.3.3. Kết luận

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

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

1.2) Mọi giao diện người sử dụng đều được mô tả trong IXIT;

1.3) Mọi API truy cập từ xa đều được mô tả trong IXIT.

2) 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

3.11.1.2.1. Mục đích kiểm thử

Đánh giá sự tuân thủ về thiết kế của thiết bị camera liên quan tới việc xử lý dữ liệu cá nhân.

3.11.1.2.2. Phương pháp kiểm thử

Phòng đo kiểm đánh giá "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.

3.11.1.2.3. Kết luận

1) Đáp ứng: Thông tin về việc xử lý dữ liệu cá nhân được cung cấp cho người sử dụng.

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

3.11.1.3. Đánh giá sự tuân thủ về triển khai

3.11.1.3.1. 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.

3.11.1.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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 đảm bảo rõ ràng đối với người sử dụng.

4) 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, đảm bảo rõ ràng đối với người sử dụng.

3.11.1.3.3. Kết luận

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

1.1) Thông tin về việc xử lý dữ liệu cá nhân được thu thập như mô tả;

1.2) Thông tin thu thập được về quá trình việc xử lý dữ liệu cá nhân tuân thủ với mô tả;

1.3) Mô tả rõ ràng và minh bạch về quá trình xử lý dữ liệu cá nhân;

1.4) Mô tả rõ ràng và minh bạch cách thức dữ liệu cá nhân đang được sử dụng, bởi ai, cho mục đích gì.

2) 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 rõ ràng và minh bạch về việc 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

3.11.2.2.1. 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.

3.11.2.2.2. Phương pháp kiểm thử

1) 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 được mô tả trong phần "Thu thập sự đồng ý":

1.1) Cho phép xác nhận một cách tự do;

1.2) Các lựa chọn được đưa ra một cách rõ ràng;

1.3) Các yêu cầu xác nhận phải minh.

3.11.2.2.3. Kết luận

1) 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:

1.1) 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;

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

2) 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

3.11.2.3.1. 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.

3.11.2.3.2. Phương pháp kiểm thử

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.

3.11.2.3.3. Kết luận

1) 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 về cách thức thu thập sự đồng ý của người sử dụng tuân thủ với mô tả.

2) 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 dịch vụ.

3.11.3.2. Đánh giá sự tuân thủ về thiết kế

3.11.3.2.1. 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.

3.11.3.2.2. Phương pháp kiểm thử

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.

3.11.3.2.3. Kết luận

1) 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 về 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.

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

3.11.3.3. Đánh giá sự tuân thủ về triển khai

3.11.3.3.1. 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.

3.11.3.3.2. Phương pháp kiểm thử

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".

3.11.3.3.3. Kết luận

1) 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, cách thức thu hồi sự đồng ý của người sử dụng tuân thủ với mô tả.

2) 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

3.11.4.2.1. 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.

3.11.4.2.2. Phương pháp kiểm thử

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.

3.11.4.2.3. Kết luận

1) Đáp ứng: Thông tin về việc xử lý dữ liệu đo đạc từ xa được cung cấp cho người sử dụng.

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

3.11.4.3. Đánh giá sự tuân thủ về triển khai

3.11.4.3.1. 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.

3.11.4.3.2. Phương pháp kiểm thử

1) 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.

2) 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.

3) 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.

4) 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.

3.11.4.3.3. Kết luận

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

1.1) Thông tin về việc xử lý dữ liệu đo đạc từ xa được thu thập như mô tả;

1.2) Thông tin về việc xử lý dữ liệu đo đạc từ xa tuân thủ với mô tả;

1.3) Dữ liệu đo đạc từ xa đang được xử lý được mô tả rõ ràng và minh bạch;

1.4) 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.

2) 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

3.11.5.2.1. 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.

3.11.5.2.2. Phương pháp kiểm thử

Đối với mỗi mô tả trong IXIT 11-ComMech và IXIT 28-ExtAPI, phòng đo kiểm đánh giá thiết bị camera có 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.

3.11.5.2.3. Kết luận

1) Đáp ứng: Có 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.

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

3.11.5.3. Đánh giá sự tuân thủ về triển khai

3.11.5.3.1. 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.

3.11.5.3.2. Phương pháp kiểm thử

1) 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.

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

3.11.5.3.3. Kết luận

1) Đáp ứng: 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.

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

4. QUY ĐỊNH VỀ QUẢN LÝ

4.1. Thiết bị camera có mức độ rủi ro trung bình, mức độ rủi ro cao thuộc phạm vi điều chỉnh quy định tại Mục 1.1 phải được công bố hợp quy theo Quy chuẩn này, gắn dấu hợp quy (dấu CR).

4.2. Công bố hợp quy

4.2.1. Việc công bố hợp quy đối với các thiết bị camera có mức độ rủi ro trung bình thuộc phạm vi của Quy chuẩn này dựa trên kết quả tự đánh giá của tổ chức, cá nhân trên cơ sở kết quả thử nghiệm của tổ chức thử nghiệm chỉ định theo quy định của pháp luật hoặc kết quả đánh giá sự phù hợp của tổ chức quốc tế, khu vực, nước ngoài được thừa nhận theo quy định.

4.2.2. Việc công bố hợp quy đối với các thiết bị camera có mức độ rủi ro cao thuộc phạm vi của Quy chuẩn này dựa trên kết quả chứng nhận hợp quy của tổ chức chứng nhận được chỉ định theo quy định của pháp luật.

4.2.3. Chứng nhận hợp quy

Việc chứng nhận sự phù hợp thực hiện theo phương thức 5 (Chứng nhận thông qua thử nghiệm mẫu đại diện cho kiểu, loại sản phẩm, hàng hóa và đánh giá quá trình sản xuất hoặc hệ thống quản lý. Giám sát thông qua thử nghiệm mẫu và đánh giá quá trình sản xuất hoặc hệ thống quản lý. Mẫu thử nghiệm trong giám sát có thể lấy tại nơi sản xuất hoặc lấy trên thị trường hoặc được lấy cả tại nơi sản xuất và trên thị trường) hoặc phương thức 7 (Chứng nhận thông qua thử nghiệm, đánh giá lô sản phẩm, hàng hóa) quy định tại các văn bản quy phạm pháp luật về công bố hợp quy. Thử nghiệm phục vụ việc chứng nhận sự phù hợp phải được thực hiện bởi tổ chức thử nghiệm được chỉ định theo quy định. Phạm vi thử nghiệm của tổ chức thử nghiệm phải đáp ứng các yêu cầu quy định của Quy chuẩn kỹ thuật này.

4.2.4. Sử dụng dấu hợp quy

Dấu hợp quy phải tuân thủ theo các quy định của pháp luật về công bố hợp quy.

5. TRÁCH NHIỆM CỦA NHÀ SẢN XUẤT, TỔ CHỨC, CÁ NHÂN

5.1. Nhà sản xuất, tổ chức, cá nhân bảo đảm thiết bị camera đáp ứng yêu cầu quy định tại Mục 2 và thực hiện quy định tại Mục 4 của Quy chuẩn này.

5.2. Nhà sản xuất, tổ chức, cá nhân có trách nhiệm cung cấp các bằng chứng về sự phù hợp của sản phẩm với Quy chuẩn này khi có yêu cầu hoặc khi được kiểm tra theo quy định đối với hàng hóa lưu thông trên thị trường.

5.3. Tổ chức đánh giá sự phù hợp khi tham gia thử nghiệm, chứng nhận sản phẩm phù hợp với Quy chuẩn này có trách nhiệm thực hiện theo quy định tại Mục 3 của Quy chuẩn này.

Phụ lục A
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

1) 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.

1.1) 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-Pswd Trang thông tin điện tử").

1.2) 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.

1.3) 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.

1.4) 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.

1.5) 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.

1.6) 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.

1.7) 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.

2) 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.

2.1) 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.

2.2) 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.

2.3) 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.

2.4) 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.

2.5) 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.

2.6) 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.

2.7) 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.

2.8) 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.

3) 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.

3.1) Xác nhận quy trình cập nhật (Có hoặc 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.

3.2) Xác nhận quản lý an toàn (Có hoặc Không): Xác nhận rằng các quy trình quản lý an toàn được mô tả trong IXIT 14-SecMgmt đã được thiết lập.

4) 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.

4.1) 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").

4.2) 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.

4.3) 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.

5) 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.

5.1) 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").

5.2) 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.

5.3) 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.

5.4) 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.

5.5) 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.

6) 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.

6.1) 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").

6.1) 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.

6.1) Khung thời gian: Khung thời gian mục tiêu để hoàn thành thủ tục.

7) 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.

7.1) 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").

7.2) 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.

7.3) 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.

7.4) 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.

7.5) 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.

7.6) 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.

7.7) 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.

7.8) 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 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.

8) 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.

8.1) 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").

8.2) 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.

8.3) 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.

8.2) 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.

8.3) 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 khôi phục 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.

9) 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.

9.1) 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 tử Serv").

9.2) 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.

9.3) Cho phép cấu hình (Có hoặc 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.

9.4) 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.

10) 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.

10.1) 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").

10.2) 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.

11) 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.

11.1) 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").

11.2) 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.

11.3) 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.

11.4) 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.

11.5) 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.

11.6) 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.

12) 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.

12.1) 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").

12.2) 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. 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.

12.3) Quy trình xử lý: Mô tả cách thức dữ liệu cá nhân được xử lý, bao gồm tất cả các bên liên quan và 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.

12.4) 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 hoặc Không). Một danh sách Cơ chế kết nối rỗng cho thấy rằng dữ liệu cá nhân không được truyền tải.

12.5) Tính nhạy cảm (Có hoặc 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.

12.6) 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.

12.7) 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.

13) 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.

13.1) 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").

13.2) Mô tả: Mô tả ngắn gọn về khả năng cảm biến.

14) 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.

14.1) 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").

14.2) 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.

14.3) Loại: Chỉ định xem cơ chế phục hồi liên quan đến kết nối mạng hay mất điện hoặc cả hai.

14.4) 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.

15) 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.

15.1) 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").

15.2) 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.

15.3) Mục đích: Mô tả ngắn gọn về mục đích thu thập dữ liệu.

16) 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.

16.1) 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").

16.2) 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.

16.3) 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.

16.4) 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.

17) 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.

17.1) 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").

17.2) Mô tả: Mô tả ngắn gọn về giao diện người sử dụng cho phép nhập liệu từ người sử dụng và chỉ ra cách người sử dụng truy cập giao diện này.

18) 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.

18.1) 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").

18.2) 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.

19) 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.

19.2) 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.

19.3) Mô tả: Mô tả phương pháp xác thực dữ liệu đầu vào 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. Đồng thời, cần chỉ ra những nguồn dữ liệu nào được phương pháp này xử lý.

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".