

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

**QCVN 135:2024/BTTTT**

**QUY CHUẨN KỸ THUẬT QUỐC GIA**

**VỀ YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN**

**CHO CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET**

***National technical regulation***

***on baseline cybersecurity requirements***

***for Surveillance Camera***

**Hà Nội - 2024**

**MỤC LỤC**

[1. QUY ĐỊNH CHUNG 7](#_Toc175121081)

[1.1. Phạm vi điều chỉnh 7](#_Toc175121082)

[1.2. Đối tượng áp dụng 7](#_Toc175121083)

[1.3. Tài liệu viện dẫn 7](#_Toc175121084)

[1.4. Chữ viết tắt 7](#_Toc175121085)

[1.5. Giải thích từ ngữ 9](#_Toc175121086)

[2. QUY ĐỊNH KỸ THUẬT 11](#_Toc175121107)

[2.1. Khởi tạo mật khẩu mặc định duy nhất 11](#_Toc175121108)

[2.2. Quản lý lỗ hổng bảo mật 11](#_Toc175121109)

[2.3. Quản lý cập nhật 11](#_Toc175121110)

[2.4. Lưu trữ các tham số nhạy cảm an toàn 12](#_Toc175121111)

[2.5. Quản lý kênh giao tiếp an toàn 12](#_Toc175121112)

[2.7. Bảo vệ dữ liệu người sử dụng 12](#_Toc175121113)

[2.8. Khả năng tự khôi phục lại hoạt động bình thường sau sự cố 13](#_Toc175121114)

[2.9. Xóa dữ liệu trên thiết bị camera 13](#_Toc175121115)

[2.10. Xác thực dữ liệu đầu vào 13](#_Toc175121116)

[2.11. Bảo vệ dữ liệu trên thiết bị camera 13](#_Toc175121117)

[3. PHƯƠNG PHÁP ĐO 14](#_Toc175121118)

[3.1. Khởi tạo mật khẩu mặc định duy nhất 14](#_Toc175121119)

[3.1.1. Nhóm kiểm thử 2.1-1 14](#_Toc175121120)

[3.1.2. Nhóm kiểm thử 2.1-2 15](#_Toc175121121)

[3.1.3. Nhóm kiểm thử 2.1-3 16](#_Toc175121122)

[3.1.4. Nhóm kiểm thử 2.1-4 18](#_Toc175121123)

[3.1.5. Nhóm kiểm thử 2.1-5 19](#_Toc175121124)

[3.2. Quản lý lỗ hổng bảo mật 20](#_Toc175121125)

[3.2.1. Nhóm kiểm thử 2.2-1 20](#_Toc175121126)

[3.3. Quản lý cập nhật 21](#_Toc175121127)

[3.3.1. Nhóm kiểm thử 2.3-1 21](#_Toc175121128)

[3.3.2. Nhóm kiểm thử 2.3-2 22](#_Toc175121129)

[3.3.3. Nhóm kiểm thử 2.3-3 23](#_Toc175121130)

[3.3.4. Nhóm kiểm thử 2.3-4 24](#_Toc175121131)

[3.3.5. Nhóm kiểm thử 2.3-5 25](#_Toc175121132)

[3.3.6. Nhóm kiểm thử 2.3-6 26](#_Toc175121133)

[3.3.7. Nhóm kiểm thử 2.3-7 27](#_Toc175121134)

[3.4. Lưu trữ các thông số bí mật an toàn 29](#_Toc175121135)

[3.4.1. Nhóm kiểm thử 2.4-1 29](#_Toc175121136)

[3.4.2. Nhóm kiểm thử 2.4-2 31](#_Toc175121137)

[3.4.3. Nhóm kiểm thử 2.4-3 32](#_Toc175121138)

[3.4.4. Nhóm kiểm thử 2.4-4 34](#_Toc175121139)

[3.5. Quản lý kênh giao tiếp an toàn 35](#_Toc175121140)

[3.5.1. Nhóm kiểm thử 2.5-1 35](#_Toc175121141)

[3.5.2. Nhóm kiểm thử 2.5-2 37](#_Toc175121142)

[3.5.3. Nhóm kiểm thử 2.5-3 39](#_Toc175121143)

[3.5.4. Nhóm kiểm thử 2.5-4 40](#_Toc175121144)

[3.6. Phòng chống tấn công thông qua các giao diện của thiết bị 41](#_Toc175121145)

[3.6.1. Nhóm kiểm thử 2.6-1 41](#_Toc175121146)

[3.6.2. Nhóm kiểm thử 2.6-2 43](#_Toc175121147)

[3.6.3. Nhóm kiểm thử 2.6-3 44](#_Toc175121148)

[3.7. Bảo vệ dữ liệu người sử dụng 46](#_Toc175121149)

[3.7.1. Nhóm kiểm thử 2.7-1 46](#_Toc175121150)

[3.7.2. Nhóm kiểm thử 2.7-2 47](#_Toc175121151)

[3.8. Khả năng tự khôi phục lại hệ thống bình thường sau sự cố 48](#_Toc175121152)

[3.8.1. Nhóm kiểm thử 2.8-1 48](#_Toc175121153)

[3.8.2. Nhóm kiểm thử 2.8-2 50](#_Toc175121154)

[3.8.3. Nhóm kiểm thử 2.8-3 52](#_Toc175121155)

[3.9. Xoá dữ liệu trên thiết bị camera 53](#_Toc175121156)

[3.9.1. Nhóm kiểm thử 2.9-1 53](#_Toc175121157)

[3.10. Xác thực dữ liệu đầu vào 55](#_Toc175121158)

[3.10.1. Nhóm kiểm thử 2.10-1 55](#_Toc175121159)

[3.11. Bảo vệ dữ liệu trên thiết bị camera 57](#_Toc175121160)

[3.11.1. Nhóm kiểm thử 2.11-1 57](#_Toc175121161)

[3.11.2. Nhóm kiểm thử 2.11-2 59](#_Toc175121162)

[3.11.3. Nhóm kiểm thử 2.11-3 60](#_Toc175121163)

[3.11.4. Nhóm kiểm thử 2.11-4 61](#_Toc175121164)

[3.11.5. Nhóm kiểm thử 2.11-5 63](#_Toc175121165)

[4. QUY ĐỊNH VỀ QUẢN LÝ 65](#_Toc175121166)

[5. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN 65](#_Toc175121167)

[6. TỔ CHỨC THỰC HIỆN 65](#_Toc175121168)

[PHỤ LỤC A 66](#_Toc175121169)

[PHỤ LỤC B 84](#_Toc175121170)

[PHỤ LỤC C 113](#_Toc175121171)

**Lời nói đầu**

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

**QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN CHO CAMERA GIÁM SÁT SỬ DỤNG GIAO THỨC INTERNET**

***National technical regulation on baseline cybersecurity requirements for Surveillance Camera***

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

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

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

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

1.2. Đối tượng áp dụng

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

1.3. Tài liệu viện dẫn

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

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

1.4. Chữ viết tắt

|  |  |  |
| --- | --- | --- |
| API | Application Programming Interface | Giao diện lập trình ứng dụng |
| ASLR | Address Space Layout Randomization | Ngẫu nhiên hóa bố trí không gian địa chỉ |
| CVD | Coordinated Vulnerability Disclosure | Công bố lỗ hổng phối hợp |
| CVRF | Common Vulnerability Reporting Framework | Khung báo cáo lỗ hổng chung |
| DDoS | Distributed Denial of Service | Tấn công từ chối dịch vụ phân tán |
| DSC | Dedicated Security Components | Các thành phần bảo mật chuyên dụng |
| EU | European Union | Liên minh Châu Âu |
| GDPR | General Data Protection Regulation | Quy định bảo vệ dữ liệu chung |
| IEEE | Institute of Electrical and Electronics Engineers | Viện Kỹ sư Điện và Điện tử |
| IoT | Internet of Things | Internet vạn vật |
| IP | Internet Protocol | Giao thức Internet |
| ISO | International Organization for Standardization | Tổ chức Tiêu chuẩn hóa Quốc tế |
| JTAG | Joint Test Action Group | Nhóm hành động thử nghiệm chung |
| LAN | Local Area Network | Mạng cục bộ |
| LoRaWAN | Long Range Wide Area Network | Mạng diện rộng tầm xa |
| MAC | Media Access Control | Điều khiển truy cập môi trường |
| NIST | National Institute of Standards and Technology | Viện Tiêu chuẩn và Công nghệ Quốc gia |
| NX | No execute | Không thực thi |
| OTP | One-Time Password | Mật khẩu dùng một lần |
| QR | Quick Response | Phản hồi nhanh |
| SBOM | Software Bill of Materials | Hóa đơn nguyên liệu phần mềm |
| SDO | Standards Development Organization | Tổ chức phát triển tiêu chuẩn |
| SE | Secure Elements | Yếu tố bảo mật |
| SSID | Service Set IDentifier | Nhận diện bộ dịch vụ |
| STRIDE | Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege | Giả mạo, Làm giả, Phủ nhận, Tiết lộ thông tin, Từ chối dịch vụ, Nâng cao đặc quyền |
| SWD | Serial Wire Debug | Gỡ lỗi dây nối tiếp |
| TEE | Trusted Execution Environment | Môi trường thực thi tin cậy |
| TS | Technical Specification | Thông số kỹ thuật |
| UART | Universal Asynchronous Receiver-Transmitter | Bộ thu phát không đồng bộ toàn cầu |
| UI | User Interface | Giao diện người dùng |
| WAN | Wide Area Network | Mạng diện rộng |

1.5. Giải thích từ ngữ

1.5.1. Dịch vụ liên kết (Associated services)

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

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

1.5.2. Chế độ cài đặt gốc (Factory default)

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

1.5.3. Chức năng cảm biến (Sensing capability)

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

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

1.5.4. Cứng hóa (Hard-code)

Lưu thông số kỹ thuật, dữ liệu được lưu trực tiếp trên mã nguồn phần mềm.

1.5.5. Dữ liệu cá nhân (Personal data)

Thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể.

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

Các thông tin thu thập trên thiết bị camera từ môi trường đánh giá để phục vụ việc khắc phục, xử lý lỗi thiết bị camera từ nhà sản xuất.

1.5.7. 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.

1.5.8. 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.

1.5.9. Giao diện gỡ lỗi (Debug interface)

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

1.5.10. Giao diện logic (Logical interface)

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

1.5.11. Giao diện mạng (Network interface)

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

1.5.12. Giao diện vật lý (Physical interface)

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

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

1.5.13. Mật khẩu khởi tạo (Initial interface)

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

1.5.14. Mật khẩu mặc định (Default password)

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

1.5.15. Quá trình khởi động (Initialization)

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

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

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

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

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

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

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

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

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

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

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

1.5.20. Truy cập từ xa (Access remotely)

Truy cập từ bên ngoài mạng nội bộ.

2. QUY ĐỊNH KỸ THUẬT

## 2.1. Khởi tạo mật khẩu mặc định duy nhất

**Yêu cầu 2.1-1** Tất cả mật khẩu mặc định được khởi tạo bởi nhà sản xuất, được sử dụng bởi camera để xác thực người dùng hoặc các dịch vụ liên kết phải là duy nhất trên mỗi thiết bị hoặc do người dùng xác định.

**Yêu cầu 2.1-2** Mật khẩu mặc định phải được tạo ra có độ phực tạp nhất định để chống lại các cuộc tấn công tự động.

**Yêu cầu 2.1-3** Các cơ chế xác thực sử dụng phương pháp mật mã an toàn, không tồn tại các điểm yếu, rủi ro an toàn thông tin tại thời điểm đánh giá.

**Yêu cầu 2.1-4** Camera có chức năng hỗ trợ người dùng hoặc quản trị viên thay đổi giá trị xác thực.

**Yêu cầu 2.1-5** Cơ chế xác thực có khả năng ngăn chặn tấn công vét cạn tự động (brute-force) qua giao diện đăng nhập.

## 2.2. Quản lý lỗ hổng bảo mật

**Yêu cầu 2.2-1** Nhà sản xuất có hệ thống trực tuyến cho phép tiếp nhận và công bố thông tin về lỗ hổng của thiết bị tới người sử dụng. Chính sách này phải bao gồm:

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

b) Thông tin thời gian tối thiểu nhà sản xuất cần để xác nhận thông tin về lỗ hổng được tiếp nhận;

c) Thông tin cập nhật trạng thái thực hiện các bước xử lý lỗ hổng.

## 2.3. Quản lý cập nhật

**Yêu cầu 2.3-1** Camera có chức năng cho phép các phần mềm trong thiết bị camera được cập nhật an toàn.

**Yêu cầu 2.3-2** Camera có chức năng hỗ trợ người dùng thực hiện cập nhật phần mềm.

**Yêu cầu 2.3-3**  Camera sử dụng cơ chế mật mã an toàn để thực hiện cập nhật

**Yêu cầu 2.3-4** Bản cập phải được nhà sản xuất công bố kịp thời.

**Yêu cầu 2.3-5** Camera có cơ chế xác thực kiểm tra tính toàn vẹn của từng bản cập nhật khi thực hiện cập nhật qua giao diện mạng.

**Yêu cầu 2.3-6** Nhà sản xuất công bố thời hạn hỗ trợ bảo hành đối với từng chủng loại thiết bị camera cung cấp ra thị trường.

**Yêu cầu 2.3-7** Camera được dán nhãn trên thiết bị hoặc qua giao diện vật lý cho phép người sử dụng tra cứu thông tin về mã, chủng loại sản phẩm thiết bị.

## 2.4. Lưu trữ các tham số nhạy cảm an toàn

**Yêu cầu 2.4-1** Các tham số nhạy cảm an toàn phải được lưu trữ một cách an toàn/mã hóa trên bộ nhớ của thiết bị.

**Yêu cầu 2.4-2** Thông số kỹ thuật cứng hoá được lưu trên thiết bị camera không cho phép người sử dụng thay đổi.

**Yêu cầu 2.4-3** Các tham số nhạy cảm an toàn không được lưu trữ trên mã nguồn của thiết bị camera.

**Yêu cầu 2.4-4** Tham số nhạy cảm an toàn được sử dụng để kiểm tra tính nguyên vẹn và tính xác thực của các bản cập nhật phần mềm hoặc để bảo vệ giao tiếp với các dịch vụ liên kết, phải là duy nhất cho mỗi thiết bị, được tạo ngẫn nhiên và có yêu cầu về độ phức tạp đối với tham số bảo mật bí mật được sinh ra.

## 2.5. Quản lý kênh giao tiếp an toàn

**Yêu cầu 2.5-1** Phương pháp mã hóa sử dụng trong các kênh giao tiếp không tồn tại lỗ hổng, điểm yếu an toàn thông tin mạng được công bố bởi các cơ quan, tổ chức trong nước hoặc nước ngoài tại thời điểm đánh giá.

**Yêu cầu 2.5-2** 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.

**CHÚ THÍCH:** Yêu cầu này không áp dụng đối với các dịch vụ hệ thống, phục vụ hoạt động của thiết bị camera như: ARP; DHCP; DNS; ICMP; NTP;...

**Yêu cầu 2.5-3** Tham số nhạy cảm an toàn khi truyền qua môi trường mạng phải sử dụng kênh giao tiếp an toàn.

**Yêu cầu 2.5-4** Nhà sản xuất công bố và tuân thủ quy trình quản lý các thông số bảo mật bí mật được sử dụng bởi thiết bị camera.

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

**Yêu cầu 2.6-1** Tất cả các giao diện mạng và logic không sử dụng phải được vô hiệu hóa.

**Yêu cầu 2.6-2** Ở trạng thái hoạt động ban đầu, khi người sử dụng chưa được xác thực, tất cả các giao diện quản trị của thiết bị không cung cấp thông tin liên quan đến thông số bảo mật bí mật và thông số bảo mật nhạy cảm của camera.

**Yêu cầu 2.6-3** Camera có chức năng vô hiệu hóa giao diện gỡ lỗi có thể truy cập vật lý, bằng phần mềm.

## 2.7. Bảo vệ dữ liệu người sử dụng

**Yêu cầu 2.7-1** Dữ liệu cá nhân thu thập, xử lý bởi thiết bị camera được truyền giữa thiết bị và các dịch vụ liên quan phải sử dụng kênh kết nối được mã hóa an toàn.

**Yêu cầu 2.7-2** Tất cả các chức năng cảm biến của camera được mô tả trong tài liệu đặc tả kỹ thuật.

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

**Yêu cầu 2.8-1** Camera có chức năng cho phép khôi phục lại hoạt động bình thường khi xảy ra sự cố mất điện hoặc mất kết nối mạng.

**Yêu cầu 2.8-2** Camera hoạt động bình thường đối với các chức năng nội bộ khi bị mất kết nối mạng và khôi phục hoạt động bình thường khi kết nối mạng được khôi phục.

**Yêu cầu 2.8-3** Khi camera khôi phục kết nối mạng, việc khôi phục lại kết nối từ camera đến các dịch vụ liên kết được thực hiện tuần tự, tránh xung đột mạng.

## 2.9. Xóa dữ liệu trên thiết bị camera

**Yêu cầu 2.9-1** Camera có chức năng cho phép người sử dụng xóa dữ liệu cá nhân và cấu hình hệ thống được thu thập và lưu trữ trên thiết bị camera.

## 2.10. Xác thực dữ liệu đầu vào

**Yêu cầu 2.10-1** Camera phải kiểm tra tính hợp lệ của dữ liệu đầu vào trước khi xử lý, thông qua các giao diện người sử dụng, giao diện lập trình ứng dụng (APIs) hoặc giữa các dịch vụ liên kết và thiết bị.

## 2.11. Bảo vệ dữ liệu trên thiết bị camera

**Yêu cầu 2.11-1** Nhà sản xuất phải cung cấp đầy đủ thông tin về mục đích, các 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).

**Yêu cầu 2.11-2** Camera có chức năng cho phép xác nhận việc đồng ý của người sử dụng đối với việc cho phép camera thu thập và xử lý dữ liệu cá nhân.

**Yêu cầu 2.11-3** Camera có chức năng cho phép xác nhận việc hủy đồng ý của người sử dụng về về việc cho phép camera thu thập và xử lý dữ liệu cá nhân.

**Yêu cầu 2.11-4** Dữ liệu đo đạc từ xa trên thiết bị camera được thu thập bởi nhà sản xuất (nếu có) phải được mô tả đầy đủ về mục đích, đối tượng thu thập và nơi lưu trữ.

**Yêu cầu 2.11-5** Camera và các dịch vụ liên kết có tính năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

3. PHƯƠNG PHÁP ĐO

## 3.1. Khởi tạo mật khẩu mặc định duy nhất

### 3.1.1. Nhóm kiểm thử 2.1-1

**3.1.1.0. 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 Quy chuẩn này.

**3.1.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc tất cả mật khẩu mặc định được khởi tạo bởi nhà sản xuất và được camera sử dụng để xác thực người dùng hoặc các dịch vụ liên kết, phải là duy nhất trên mỗi thiết bị hay không.

**b) Phương pháp đánh giá**

Đánh giá tất cả các cơ chế xác thực dựa trên mật khẩu trong **IXIT 1-AuthMech** dựa vào các thông tin “Giá trị xác thực”và “Cơ chế khởi tạo mật khẩu”có đảm bảo rằng mật khẩu là duy nhất trên mỗi thiết bị hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Tài liệu kiểm thử mô tả và minh chứng mỗi mật khẩu được tạo bởi một cơ chế xác thực dựa trên mật khẩu là duy nhất trên mỗi thiết bị.

ii. Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

**3.1.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm thử bằng thực nghiệm để đánh giá thiết bị camera có chức năng đáp ứng yêu cầu 2.1-1, điều 2.1 Quy chuẩn này, như được mô tả trong **IXIT 1-AuthMech** hay không.

**b) Phương pháp đánh giá**

i. Đánh giá thực nghiệm xem chức năng khởi tạo mật khẩu mặc định duy nhất có đáp ứng như được mô tả trong tài liệu trong **IXIT 1-AuthMech** hoặc trong hướng dẫn sử dụng hay không.

ii. Đối với mỗi cơ chế xác thực dựa trên mật khẩu của người dùng trong **IXIT 1-AuthMech**, kiểm tra chức năng của sản phẩm được đánh giá liệu người dùng có bắt buộc phải định nghĩa tất cả các mật khẩu mà người dùng định nghĩa theo “Giá trị xác thực”trước khi được sử dụng hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Sản phẩm được đánh giá có chức năng đáo ứng các yêu cầu, bao gồm:

* Mỗi cơ chế xác thực dựa trên mật khẩu được được mô tả trong **IXIT** được đánh giá đầy đủ;
* Kết quả đánh giá cho thấy thiết bị camera khởi tạo mật khẩu mặc định duy nhất như được mô tả trong bảng **IXIT 1-AuthMech**.

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

### 3.1.2. Nhóm kiểm thử 2.1-2

**3.1.2.0. 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 Quy chuẩn này.

**3.1.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc mật khẩu mặc định phải được tạo ra có độ phực tạp nhất định để chống lại các cuộc tấn công tự động.

**b) Phương pháp đánh giá**

i. Đánh giá “Cơ chế khởi tạo mật khẩu” trong **IXIT 1-AuthMech** có mô tả đầy đủ các quy tắc khởi tạo mật khẩu hay không.

ii. Đánh giá liệu cơ chế tạo mật khẩu có tạo ra các chuỗi mật khẩu thông dụng hay không. Chuỗi mật khẩu thông dùng bao gồm, nhưng không giới hạn các mật khẩu tại đường dẫn dưới đây: <https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt>.

iii. Đánh giá liệu cơ chế tạo mật khẩu có tạo ra các mật khẩu chứa các thông tin công khai hay không, bao gồm nhưng không giới hạn các thông tin địa chỉ MAC, SSID Wi-Fi®, tên, loại và mô tả của thiết bị.

iv. Đánh giá liệu cơ chế tạo mật khẩu có tạo ra các mật khẩu đáp ứng các yêu cầu về độ phức tạp hay không.

**c) Kết luận đánh giá**

i. Đáp ứng:Tài liệu kiểm thử mô tả đầy đủ các thông tin, bao gồm:

* Mô tả đầy đủ các cơ chế tạo mật khẩu;
* Cơ chế tạo mật khẩu minh chứng không tìm thấy các chuỗi thông dụng;
* Các cơ chế tạo mật khẩu không tạo ra các mật khẩu có liên quan đến thông tin công khai;
* Các cơ chế tạo mật khẩu đáp ứng các yêu cầu về độ phức tạp.

ii. Không đáp ứng: Nếu một trong các yêu cầu ở trên không đáp ứng.

**3.1.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm thử bằng thực nghiệm để đánh giá thiết bị camera có chức năng đáp ứng yêu cầu 2.1-2, điều 2.1 Quy chuẩn này, như được mô tả trong **IXIT 1-AuthMech** hay không.

**b) Phương pháp đánh giá**

i. Kiểm thử mỗi mật khẩu theo mô tả trong “Giá trị xác thực”được tạo bởi “Cơ chế khởi tạo mật khẩu”trong **IXIT 1-AuthMech** có đáp ứng yêu cầu về độ phực tạp hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Mỗi mật khẩu theo mô tả trong “Giá trị xác thực”được tạo bởi “Cơ chế khởi tạo mật khẩu”trong **IXIT 1-AuthMech** đáp ứng yêu cầu về độ phực tạp.

ii. Không đáp ứng: Nếu yêu cầu ở trên không đáp ứng.

### 3.1.3. Nhóm kiểm thử 2.1-3

**3.1.3.0. 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 Quy chuẩn này.

**3.1.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc các cơ chế xác thực sử dụng phương pháp mật mã an toàn, không tồn tại các điểm yếu, rủi ro an toàn thông tin tại thời điểm đánh giá.

**b) Phương pháp đánh giá**

i. Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech**, đánh giá các "Điều kiện đảm bảo bảo mật" có bảo đảm các yêu cầu về tính toàn vẹn và xác thực.

ii. Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech**, đánh giá cơ chế xác thực có phù hợp với các "Điều kiện đảm bảo bảo mật" hay không.

iii. Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech**, đánh giá "Phương thức mã hóa" có sử dụng phương pháp mật mã an toàn, không tồn tại các điểm yếu, rủi ro an toàn thông tin tại thời điểm đánh giá hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Tài liệu kiểm thử mô tả đầy đủ các thông tin, bao gồm:

* Các "Điều kiện đảm bảo bảo mật" bảo đảm các yêu cầu về tính toàn vẹn và xác thực;
* Cơ chế xác thực trong **IXIT 1-AuthMech** phù hợp với các "Điều kiện đảm bảo bảo mật";
* Phương thức mã hóa sử dụng phương pháp mật mã an toàn, không tồn tại các điểm yếu, rủi ro an toàn thông tin tại thời điểm đánh giá.

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

**3.1.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm thử bằng thực nghiệm để đánh giá thiết bị camera có chức năng đáp ứng yêu cầu 2.1-3, điều 2.1 Quy chuẩn này, như được mô tả trong **IXIT 1-AuthMech** hay không.

**b) Phương pháp đánh giá**

Đối với mỗi cơ chế xác thực trong **IXIT 1-AuthMech**, đánh giá cụ thể các "Phương thức mã hoá" sử dụng có đáp ứng yêu cầu an toàn hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Đánh giá bằng thực nghiệm minh chứng được "Phương thức mã hoá" sử dụng có đáp ứng yêu cầu an toàn.

ii. Không đáp ứng: Nếu yêu cầu ở trên không đáp ứng.

### 3.1.4. Nhóm kiểm thử 2.1-4

**3.1.4.0. 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 Quy chuẩn này.

**3.1.4.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng hỗ trợ người dùng hoặc quản trị viên thay đổi giá trị xác thực.

**b) Phương pháp đánh giá**

Đánh giá mô tả về “Giá trị xác thực” trong bảng **IXIT 1-AuthMech** và "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo** có hướng dẫn thay đổi giá trị xác thực qua giao diện đồ hoạ hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Mô tả về “Giá trị xác thực” trong bảng **IXIT 1-AuthMech** và "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo** có hướng dẫn thay đổi giá trị xác thực qua giao diện đồ hoạ.

ii. Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

**3.1.4.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm thử bằng thực nghiệm để đánh giá thiết bị camera có chức năng đáp ứng yêu cầu 2.1-4, điều 2.1 Quy chuẩn này hay không.

**b) Phương pháp đánh giá**

Kiểm thử bằng thực nghiệm để minh chứng các giá trị xác thực như được thay đổi thành công như được mô tả trong mục "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo**.

**c) Kết luận đánh giá**

i. Đáp ứng: Các giá trị xác thực như được thay đổi thành công như được mô tả trong mục "Tài liệu hướng dẫn thay đổi thông tin xác thực" trong **IXIT 2-UserInfo**.

ii. Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

### 3.1.5. Nhóm kiểm thử 2.1-5

**3.1.5.0. 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 Quy chuẩn này.

**3.1.5.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc cơ chế xác thực được sử dụng bởi camera có khả năng ngăn chặn tấn công vét cạn tự động brute-force qua giao diện mạng.

**b) Phương pháp đánh giá**

Đánh giá mỗi cơ chế xác thực trong **IXIT 1-AuthMech** có mô tả phương pháp ngăn chặn tấn công vét cạn qua giao diện mạng hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: Tài liệu kiểm thử có mô tả phương pháp ngăn chặn tấn công vét cạn qua giao diện mạng.

ii. Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

**3.1.5.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm thử bằng thực nghiệm để đánh giá thiết bị camera có chức năng đáp ứng yêu cầu 2.1-5, điều 2.1 Quy chuẩn này, như được mô tả trong **IXIT 1-AuthMech** hay không.

**b) Phương pháp đánh giá**

Đánh giá chức năng ngăn chặn tấn công vét cạn được mô tả trong **IXIT 1-AuthMech**.

**c) Kết luận đánh giá**

i. Đáp ứng: Sản phẩm được đánh giá và minh chứng có chức năng ngăn chặn tấn công vét cạn được mô tả trong **IXIT 1-AuthMech**.

ii. Không đáp ứng: Nếu yêu cầu trên không đáp ứng.

## 3.2. Quản lý lỗ hổng bảo mật

### 3.2.1. Nhóm kiểm thử 2.2-1

**3.2.1.0. 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 Quy chuẩn này.

**3.2.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc nhà sản xuất có hệ thống trực tuyến cho phép tiếp nhận và công bố thông tin về lỗ hổng của thiết bị tới người sử dụng.

**b) Phương pháp đánh giá**

Đánh giá tài liệu kiểm thử có mô tả về "Chính sách công bố lỗ hổng" trong bảng **IXIT 2-UserInfo** hay không.

**c) Kết luận đánh giá**

i. Đáp ứng: nếu bảng **IXIT 2-UserInfo** có mô tả "Chính sách công bố lỗ hổng" của nhà sản xuất được công bố và truy cập công khai.

ii. Không đáp ứng: Nếu không đáp ứng yêu cầu trên.

**3.2.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Đánh giá nhà sản xuất có và thực hiện chính sách công bố lỗ hổng bảo mật hay không.

**b) Phương pháp đánh giá**

i. Đánh giá nhà sản xuất có hệ thống trực tuyến và thực hiện chính sách công bố lỗ hổng bảo mật như được mô tả trong bảng **IXIT 2-UserInfo** hay không.

ii. Kiểm thử chính sách và hệ thống trực tuyến có cung cấp đầy đủ thông tin bao gồm:

* Thông tin liên hệ để tiếp nhận thông tin về lỗ hổng;
* Thông tin thời gian tối thiểu nhà sản xuất cần để xác nhận thông tin về lỗ hổng được tiếp nhận;
* Thông tin cập nhật trạng thái thực hiện các bước xử lý lỗ hổng.

**c) Kết luận đánh giá**

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

* Chính sách công bố lỗ hổng bảo mật có thể truy cập công khai;
* Chính sách công bố lỗ hổng bảo mật bao gồm các thông tin như ở trên.

ii. **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 2.3-1

**3.3.1.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-1, điều 2.3 Quy chuẩn này.

**3.3.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng cho phép các phần mềm trong thiết bị camera được cập nhật an toàn.

**b) Phương pháp đánh giá**

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 “Điều kiện đảm bảo bảo mật”, "Mô tả", "Phương thức mã hóa" và "Khởi tạo và tương tác" hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** Tài liệu kiểm thử có mô tả cơ chế cập nhật có khả năng ngăn chặn được các hình thức tấn công mạng dựa vào các mô tả tại “Điều kiện đảm bảo bảo mật”, "Mô tả", "Phương thức mã hóa" và "Khởi tạo và tương tác".

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.3.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của kịch bản kiểm thử này là đánh giá chức năng cập nhật có khả năng ngăn chặn được các hình thức tấn công mạng hay không.

**b) Phương pháp đánh giá**

i. Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, thực hiện các kịch bản tấn công dựa trên phần "Mô tả".

**Ví dụ 1:** Thực hiện tấn công Man-In-The-Middle (MITM) giữa thiết bị camera và máy chủ cập nhật.

ii. Dựa vào thông tin được mô tả tại phần "Mô tả", "Phương thức mã hóa" và "Khởi tạo và tương tác" để tìm ra các điểm yêu của mỗi cơ chế cập nhật từ đó thực hiện cách tấn công khai thác để đánh giá chức năng cập nhật có khả năng ngăn chặn được các hình thức tấn công mạng hay không.

**Ví dụ 2:** Nếu một cơ chế cập nhật dựa trên chữ ký số của tập tin để xác minh tính hợp lệ, người đánh giá có thể tạo ra các tệp tin giả mạo để kiểm tra xem cơ chế cập nhật có khả năng phát hiện và ngăn chặn hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** Các hình thức tấn công để khai thác điểm yếu của cơ chế cập nhật không thành công.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.3.2. Nhóm kiểm thử 2.3-2

**3.3.2.0. 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 Quy chuẩn này.

**3.3.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng hỗ trợ người dùng thực hiện cập nhật phần mềm.

**b) Phương pháp đánh giá**

Đối với mỗi thành phần phần mềm, dựa vào mô tả về "Cơ chế cập nhật" trong **IXIT 6-SoftComp**, và "Khởi tạo và tương tác" trong **IXIT 7-UpdMech** để đánh giá camera có chức năng hỗ trợ người dùng thực hiện cập nhật phần mềm đáp ứng tối thiểu một trong các yêu cầu sau:

* Bản cập nhật phần mềm được áp dụng tự động mà không yêu cầu bất kỳ sự tương tác nào từ người dùng; hoặc
* Bản cập nhật phần mềm được khởi tạo thông qua một dịch vụ liên quan; hoặc
* Bản cập nhật phần mềm được khởi tạo thông qua giao diện web trên thiết bị; hoặc
* Bản cập nhật phần mềm sử dụng một phương pháp tương tự phù hợp với người dùng có kiến thức kỹ thuật hạn chế.

**c) Kết luận đánh giá**

i. **Đáp ứng:** Nếu mỗi thành phần phần mềm được camera hỗ trợ ít nhất một cơ chế cập nhật, mà đơn giản để người dùng áp dụng.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.3.3. Nhóm kiểm thử 2.3-3

**3.3.3.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-3, điều 2.3 Quy chuẩn này.

**3.3.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera sử dụng cơ chế mật mã an toàn để thực hiện cập nhật.

**b) Phương pháp đánh giá**

i. Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, đánh giá tài liệu kiểm thử có mô tả các “Điều kiện đảm bảo bảo mật” phù hợp để các bản cập nhật bảo đảm tính toàn vẹn và xác thực.

ii. Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, đánh giá liệu cơ chế này theo "Mô tả" có phù hợp với các “Điều kiện đảm bảo bảo mật” hay không.

iii. Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, đánh giá liệu "Phương thức mã hóa" không tồn tại lỗ hổng, điểm yếu an toàn thông tin tại thời điểm đánh giá hay không.

iv. Đối với mỗi cơ chế cập nhật trong **IXIT 7-UpdMech**, đánh giá liệu "Phương thức mã hóa" đáp ứng các “Điều kiện đảm bảo bảo mật” thì có khả năng phòng, chống các dạng tấn công mạng hay không.

**c) Kết luận đánh giá**

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

* Các “Điều kiện đảm bảo bảo mật” phù hợp để các bản cập nhật được cập nhật an toàn; và
* Cơ chế cập nhật phù hợp để để các bản cập nhật được cập nhật an toàn; và
* Phương pháp mật mã sử dụng an toàn không tồn tại lỗ hổng, điểm yếu an toàn thông tin tại thời điểm đánh giá; và
* Phương pháp mật mã sử dụng có khả năng phóng, chóng được các dạng tấn công khai thác điểm yếu.

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

### 3.3.4. Nhóm kiểm thử 2.3-4

**3.3.4.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-4, điều 2.3 Quy chuẩn này.

**3.3.4.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc bản cập phải được nhà sản xuất công bố kịp thời.

**b) Phương pháp đánh giá**

i. Đánh giá liệu "Mô tả" và "Khung thời gian" của mỗi quy trình cập nhật bảo mật trong **IXIT 8-UpdProc** có hỗ trợ việc triển khai các bản cập nhật bảo mật một cách kịp thời hay không.

ii. Kiểm tra xem "Xác nhận quy trình cập nhật" trong **IXIT 4-Conf** có nêu rõ được xác nhận hay không.

**c) Kết luận đánh giá**

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

* Tài liệu kiểm thử mô tả quy trình quản lý cập nhật đáp ứng yêu cầu về thời gian cập nhật kịp thời; và
* Có xác nhận về cam kết tại “Xác nhận quy trình cập nhật” trong **IXIT 4-Conf** của nhà sản xuất.

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

### 3.3.5. Nhóm kiểm thử 2.3-5

**3.3.5.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-5, điều 2.3 Quy chuẩn này.

**3.3.5.1. Đánh giá tài liệu kiểm thử/Chức năng thiết bị được đánh giá**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có cơ chế xác thực kiểm tra tính toàn vẹn của từng bản cập nhật khi thực hiện cập nhật qua giao diện mạng.

**b) Phương pháp đánh giá**

i. Ápdụng các Phương pháp đánh giá a-b như được chỉ định trong Kịch bản kiểm thử 5.3-9-1.

ii. Đối với mỗi cơ chế cập nhật dựa trên mạng trong **IXIT 7-UpdMech**, đánh giá liệu việc xác minh tính toàn vẹn và tính xác thực có dựa trên một mối quan hệ tin cậy hợp lệ theo "Mô tả" và “Điều kiện đảm bảo bảo mật” hay không. Một mối quan hệ tin cậy hợp lệ bao gồm:

* Kênh truyền thông được xác thực; hoặc
* Có mặt trên một mạng yêu cầu thiết bị phải sở hữu một tham số bảo mật quan trọng hoặc mật khẩu để tham gia; hoặc
* Xác minh bằng chữ ký số của bản cập nhật; hoặc
* Xác nhận bởi người dùng; hoặc
* Một chức năng bảo mật tương đương.

iii. Đánh giá chức năng liệu các cơ chế cập nhật không được tài liệu hóa trong **IXIT 7-UpdMech** có sẵn thông qua một giao diện mạng trên thiết bị camera hay không.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Mỗi cơ chế cập nhật có minh chứng được tính xác thực của các bản cập nhật phần mềm; và
* Mỗi cơ chế cập nhật minh chứng được việc xác minh tính toàn vẹn của các bản cập nhật phần mềm; và
* Việc minh chứng tính xác thực và toàn vẹn của các bản cập nhật phần mềm dựa trên một mối quan hệ tin cậy hợp lệ; và
* Mọi cơ chế cập nhật dựa trên mạng được phát hiện đều được tài liệu hóa trong **IXIT**.

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

### 3.3.6. Nhóm kiểm thử 2.3-6

**3.3.6.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-6, điều 2.3 Quy chuẩn này.

**3.3.6.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc nhà sản xuất công bố thời hạn hỗ trợ bảo hành đối với từng chủng loại thiết bị camera cung cấp ra thị trường.

**b) Phương pháp đánh giá**

Đánh giá xem liệu thông tin "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có dễ hiểu đối với một người dùng hay không.

**Ví dụ:** Với nhãn gán trên thiết bị camera, người dùng có thể tìm thấy thời gian hỗ trợ thông qua công cụ tìm kiếm trên trang web của nhà sản xuất.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Việc công bố thời gian hỗ trợ cập nhật phần mềm dễ hiểu đối với người dùng.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.3.6.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của việc công bố thời gian hỗ trợ được định nghĩa.

**b) Phương pháp đánh giá**

i. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thông tin người dùng về cách truy cập tài nguyên để công bố thời gian hỗ trợ được định nghĩa theo "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có được cung cấp như mô tả hay không.

ii. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu nhà sản xuất công bố thời gian hỗ trợ được định nghĩa theo "Công bố thời gian hỗ trợ" trong **IXIT 2-UserInfo** có thể truy cập công khai hay không.

iii. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thời gian hỗ trợ được công bố theo "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 thể cập nhật như được mô tả trong "Thời gian Hỗ trợ" trong **IXIT 2-UserInfo** hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Truy cập vào nguồn thông tin mà nhà sản xuất công bố thời gian hỗ trợ được định nghĩa cho người dùng được cung cấp như mô tả trong **IXIT**; và
* Truy cập vào nguồn thông tin mà nhà sản xuất công bố để công bố thời gian hỗ trợ được định nghĩa được công khai; và
* Thời gian hỗ trợ được định nghĩa đã được công bố.

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

### 3.3.7. Nhóm kiểm thử 2.3-7

**3.3.7.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.3-7, điều 2.3 Quy chuẩn này.

**3.3.7.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera được dán nhãn trên thiết bị hoặc qua giao diện vật lý cho phép người sử dụng tra cứu thông tin về mã, chủng loại sản phẩm thiết bị.

**b) Phương pháp đánh giá**

Đánh giá định danh 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 "Định danh thiết bị" trong **IXIT 2-UserInfo**.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Tên mô hình của thiết bị camera có thể được nhận dạng rõ ràng thông qua việc gán nhãn trên thiết bị camera hoặc thông qua một giao diện vật lý.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.3.7.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của việc định danh thiết bị camera.

**b) Phương pháp đánh giá**

i. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu tên mô hình của thiết bị camera có thể được nhận dạng bằng cách áp dụng phương pháp nhận dạng được mô tả trong "Định danh thiết bị" trong **IXIT 2-UserInfo** hay không.

ii. Đánh giá chức năng liệu tên mô hình thu được có sẵn dưới dạng văn bản đơn giản và có khớp với tên mô hình dự kiến được mô tả trong "Định danh thiết bị" trong **IXIT 2-UserInfo** hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Định danh của Thiết bị camera có thể được trích xuất theo cách nhận dạng được mô tả
* Tên mô hình có sẵn dưới dạng văn bản đơn giản
* Tên mô hình khớp với tên mô hình dự kiến theo **IXIT**.

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

## 3.4. Lưu trữ các thông số bí mật an toàn

### 3.4.1. Nhóm kiểm thử 2.4-1

**3.4.1.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4-1, điều 2.4 Quy chuẩn này.

**3.4.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc các tham số bảo mật bí mật phải lưu trữ mã hóa trên bộ nhớ của thiết bị.

**b) Phương pháp đánh giá**

i. Đánh giá liệu tuyên bố trong "Loại" của mỗi tham số bảo mật nhạy cảm được cung cấp trong **IXIT 10-SecParam** có nhất quán với "Mô tả" hay không.

ii. Đánh giá liệu “Điều kiện đảm bảo bảo mật” của mỗi tham số bảo mật nhạy cảm được cung cấp trong **IXIT 10-SecParam** có khớp với ít nhất các yêu cầu bảo vệ được chỉ định bởi "Loại" hay không.

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

iii. Đánh giá liệu "Biện pháp bảo vệ" của mỗi tham số bảo mật nhạy cảm được cung cấp trong **IXIT 10-SecParam** có cung cấp các "Điều kiện đảm bảo bảo mật" đã được tuyên bố hay không.

iv. Đánh giá tính đầy đủ của các tham số bảo mật nhạy cảm trong **IXIT 10-SecParam** bằng cách xem xét các chỉ dẫn về các tham số bảo mật nhạy cảm trong thông tin được cung cấp trong tất cả các **IXIT** khác.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Đối với mọi tham số bảo mật nhạy cảm, tuyên bố nhất quán với mô tả của nó; và
* Đối với mọi tham số bảo mật nhạy cảm, các đảm bảo bảo mật được tuyên bố khớp với các yêu cầu bảo vệ tối thiểu của chúng; và
* Mỗi tham số bảo mật nhạy cảm có một cơ chế bảo vệ phù hợp cho các đảm bảo bảo mật đã tuyên bố; và
* Không có chỉ dẫn cho thấy các tham số bảo mật nhạy cảm được liệt kê là không đầy đủ.

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

**3.4.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng việc lưu trữ an toàn các tham số bảo mật nhạy cảm.

**b) Phương pháp đánh giá**

Đánh giá chức năng liệu tất cả các tham số bảo mật nhạy cảm được cung cấp trong **IXIT 10-SecParam** có "Biện pháp bảo vệ" được triển khai theo tài liệu **IXIT** này hay không.

**CHÚ THÍCH:** Thông thường, trong khi kiểm tra **Thiết bị camera** để chỉ ra các bằng chứng cho sự tồn tại và thực thi của cơ chế bảo vệ được tài liệu hóa cho một tham số bảo mật nhạy cảm, có thể tìm thấy một chỉ dẫn cho sự không tuân thủ của việc triển khai, nếu tồn tại ở mức cơ bản.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Đối với mọi tham số bảo mật nhạy cảm, không có chỉ dẫn cho thấy việc triển khai cơ chế bảo vệ tương ứng khác biệt so với tài liệu **IXIT**.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.4.2. Nhóm kiểm thử 2.4-2

**3.4.2.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4-2, điều 2.4 Quy chuẩn này.

**3.4.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc thông số kỹ thuật cứng hoá được lưu trên thiết bị camera không cho phép người sử dụng thay đổi.

**b) Phương pháp đánh giá**

i. Kiểm tra liệu đối với mỗi tham số bảo mật nhạy cảm trong **IXIT 10-SecParam** mà "Mô tả" cho thấy nó được sử dụng như một định danh mã hóa cứng, có một tuyên bố rõ ràng tương ứng được cung cấp hay không.

ii. Đánh giá liệu đối với mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam**, “Điều kiện đảm bảo bảo mật” tương ứng có cung cấp khả năng chống giả mạo hay không.

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

**CHÚ THÍCH 2:** Xem xét việc sử dụng bằng chứng bên ngoài để (một phần) bao phủ quy định nếu một phần tử bảo mật được sử dụng.

iii. Đánh giá liệu "Biện pháp bảo vệ" của mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam** có cung cấp các "Điều kiện đảm bảo bảo mật" đã tuyên bố liên quan đến khả năng chống giả mạo hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Không có chỉ dẫn cho thấy bất kỳ định danh mã hóa cứng nào không được tài liệu hóa như vậy
* Đối với tất cả các định danh mã hóa cứng, đảm bảo bảo mật bao gồm khả năng chống giả mạo
* Mỗi định danh mã hóa cứng có một cơ chế bảo vệ phù hợp cho khả năng chống giả mạo.

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

**3.4.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng việc lưu trữ chống giả mạo của các định danh mã hóa cứng.

**b) Phương pháp đánh giá**

Đánh giá chức năng liệu đối với mỗi định danh mã hóa cứng như được chỉ ra trong "Mô tả" trong **IXIT 10-SecParam**, "Biện pháp bảo vệ" liên quan đến khả năng chống giả mạo được triển khai theo tài liệu **IXIT** hay không.

**CHÚ THÍCH:** Thông thường, trong khi kiểm tra **Thiết bị camera** để chỉ ra các bằng chứng cho sự tồn tại và thực thi của cơ chế bảo vệ được tài liệu hóa cho một tham số bảo mật nhạy cảm, có thể tìm thấy một chỉ dẫn cho sự không tuân thủ của việc triển khai, nếu tồn tại ở mức cơ bản.

**Ví dụ:** Nếu "Biện pháp bảo vệ" tuyên bố rằng một định danh mã hóa cứng được bảo vệ chống giả mạo bằng một phần tử bảo mật, việc xác minh sự tồn tại và tích hợp đúng của phần tử bảo mật có thể hữu ích để thu thập một chỉ dẫn.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Đối với mọi định danh mã hóa cứng, không có chỉ dẫn cho thấy việc triển khai bất kỳ cơ chế bảo vệ nào liên quan đến khả năng chống giả mạo khác biệt so với tài liệu **IXIT**.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.4.3. Nhóm kiểm thử 2.4-3

**3.4.3.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4-3, điều 2.4 Quy chuẩn này.

**3.4.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc các tham số bảo mật bí mật không được lưu trữ trên mã nguồn của thiết bị camera.

**b) Phương pháp đánh giá**

i. Kiểm tra liệu đối với tất cả các tham số bảo mật quan trọng được cung cấp trong **IXIT 10-SecParam** mà "Cơ chế cung cấp" chỉ ra rằng nó được mã hóa cứng trong mã nguồn phần mềm của thiết bị, thực tế này có được phản ánh trong "Mô tả" hay không.

ii. Đánh giá liệu đối với tất cả các tham số bảo mật quan trọng trong **IXIT 10-SecParam**, mà được mã hóa cứng trong mã nguồn phần mềm của thiết bị theo "Mô tả", "Cơ chế cung cấp" tương ứng có đảm bảo rằng nó không được sử dụng trong quá trình hoạt động của thiết bị camera hay không.

**CHÚ THÍCH:** Theo định nghĩa của tham số bảo mật quan trọng trong ETSI TS 103 645 [1]/ETSI EN 303 645 [2], việc tiết lộ hoặc sửa đổi một tham số như vậy có thể làm suy yếu tính bảo mật của **Thiết bị camera**. Các tham số mà việc tiết lộ hoặc sửa đổi chỉ làm suy yếu các tài sản khác (ví dụ: tài sản trí tuệ) không được bao phủ bởi định nghĩa này.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Không có chỉ dẫn cho thấy bất kỳ tham số bảo mật quan trọng nào được mã hóa cứng trong mã nguồn phần mềm của thiết bị không được tài liệu hóa như vậy; và
* Đối với tất cả các tham số bảo mật quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị, "Cơ chế cung cấp" đảm bảo rằng nó không được sử dụng trong quá trình hoạt động của thiết bị camera.

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

**3.4.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng các tham số bảo mật quan trọng được mã hóa cứng.

**b) Phương pháp đánh giá**

Đánh giá chức năng liệu đối với tất cả các tham số bảo mật quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị được tài liệu hóa trong "Mô tả" của **IXIT 10-SecParam**, "Cơ chế cung cấp" có thực sự được áp dụng trong quá trình hoạt động của thiết bị camera hay không.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Đối với tất cả các tham số bảo mật quan trọng được mã hóa cứng trong mã nguồn phần mềm của thiết bị, không có chỉ dẫn cho thấy việc áp dụng cơ chế cung cấp khác biệt so với tài liệu **IXIT**.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.4.4. Nhóm kiểm thử 2.4-4

**3.4.4.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.4-4, điều 2.4 Quy chuẩn này.

**3.4.4.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc tham số bảo mật bí mật được sử dụng để kiểm tra tính nguyên vẹn và tính xác thực của các bản cập nhật phần mềm hoặc để bảo vệ giao tiếp với các dịch vụ liên kết, phải là duy nhất cho mỗi thiết bị, được tạo ngẫn nhiên và có yêu cầu về độ phức tạp đối với tham số bảo mật bí mật được sinh ra.

**b) Phương pháp đánh giá**

i. Kiểm tra liệu tất cả các tham số bảo mật quan trọng được cung cấp trong **IXIT 10-SecParam**, nơi "Mô tả" cho thấy rằng các tham số bảo mật quan trọng được sử dụng cho kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm hoặc cho bảo vệ giao tiếp với các dịch vụ liên quan có được tài liệu hóa như vậy trong "Cơ chế khởi tạo" hay không.

ii. Đánh giá liệu đối với tất cả các tham số bảo mật quan trọng được cung cấp trong **IXIT 10-SecParam**, "Cơ chế khởi tạo" có đảm bảo rằng tham số bảo mật 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.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Tất cả các tham số bảo mật quan trọng mà mục đích trong "Mô tả" cho thấy rằng các tham số bảo mật quan trọng được sử dụng cho kiểm tra tính toàn vẹn và tính xác thực của các bản cập nhật phần mềm hoặc cho bảo vệ giao tiếp với các dịch vụ liên quan được tài liệu hóa như vậy trong "Cơ chế khởi tạo"; và
* Đối với tất cả các tham số bảo mật quan trọng, "Cơ chế khởi tạo" đảm bảo rằng các tham số bảo mật 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.

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

## 3.5. Quản lý kênh giao tiếp an toàn

### 3.5.1. Nhóm kiểm thử 2.5-1

**3.5.1.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5-1, điều 2.5 Quy chuẩn này.

**3.5.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc phương pháp mã hóa sử dụng trong các kênh giao tiếp không tồn tại lỗ hổng, điểm yếu an toàn thông tin mạng được công bố bởi các cơ quan, tổ chức trong nước hoặc nước ngoài tại thời điểm đánh giá.

**b) Phương pháp đánh giá**

i. Đối với mỗi cơ chế giao tiếp trong **IXIT 11-ComMech**, đánh giá liệu “Điều kiện đảm bảo bảo mật” có phù hợp với trường hợp sử dụng của giao tiếp hay không.

ii. Đối với mỗi cơ chế giao tiếp trong **IXIT 11-ComMech**, đánh giá liệu cơ chế theo "Mô tả" có phù hợp để đạt được “Điều kiện đảm bảo bảo mật” hay không.

iii. Đối với mỗi cơ chế giao tiếp trong **IXIT 11-ComMech**, đánh giá liệu "Phương thức mã hóa" có được coi là mật mã thực hành tốt nhất 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 thực hành tốt nhất 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.

iv) Đối với mỗi cơ chế giao tiếp trong **IXIT 11-ComMech**, đánh giá liệu "Phương thức mã hóa" không dễ bị tấn công khả thi đối với tính chất bảo mật mong muốn trên cơ sở “Điều kiện đảm bảo bảo mật” bằng cách tham chiếu các báo cáo mật mã học.

**c) Kết luận đánh giá**

i. **Đáp ứng:** được đưa ra nếu đối với tất cả các cơ chế giao tiếp:

* Các đảm bảo bảo mật phù hợp với trường hợp sử dụng giao tiếp an toàn; và
* Cơ chế phù hợp để đạt được các đảm bảo bảo mật liên quan đến trường hợp sử dụng; và
* Tất cả các chi tiết mật mã được sử dụng được coi là mật mã thực hành tốt nhất cho trường hợp sử dụng; và
* Tất cả các chi tiết mật mã được sử dụng không được biết là dễ bị tấn công khả thi đối với tính chất bảo mật mong muốn.

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

**3.5.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

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

**b) Phương pháp đánh giá**

Đối với mỗi cơ chế giao tiếp trong **IXIT 11-ComMech**, đánh giá chức năng liệu "Phương thức mã hóa" đã được mô tả có được Thiết bị camera sử dụng hay không.

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

**Ví dụ 2:** Nếu sử dụng giao tiếp được bảo mật TLS, việc thu thập bắt tay TLS và so sánh các bộ mật mã đã sử dụng với mật mã được mô tả trong IXIT có thể hữu ích để thu thập một chỉ dẫn.

**Ví dụ 3:** Nếu giao thức cho phép các chế độ bảo mật khác nhau cho giao tiếp, cố gắng hạ cấp chế độ bảo mật có thể hữu ích để thu thập một chỉ dẫn.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Không có chỉ dẫn cho thấy bất kỳ cài đặt mật mã nào được sử dụng khác biệt so với tài liệu IXIT.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.5.2. Nhóm kiểm thử 2.5-2

**3.5.2.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5-2, điều 2.5 Quy chuẩn này.

**3.5.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

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

**b) Phương pháp đánh giá**

Ap dụng tất cả các phương pháp đánh giá được nêu trong Kịch bản kiểm thử 3.5-4-1 cho tất cả các trường hợp với sự hạn chế đối với các chức năng cho phép thay đổi liên quan đến bảo mật 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.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Ít nhất một cơ chế xác thực được tham chiếu cho mỗi chức năng của thiết bị có thể truy cập thông qua giao diện mạng cho phép thay đổi liên quan đến bảo mật; và
* 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 danh tính không hợp lệ và/hoặc các yếu tố xác thực; và
* Các phương tiện được sử dụng để bảo vệ một cơ chế xác thực cung cấp các đảm bảo bảo mật mong đợi và có khả năng chống lại các nỗ lực xâm phạm cơ chế; và
* Mọi cơ chế ủy quyền cho phép truy cập đối với các đối tượng đã xác thực với quyền truy cập thích hợp; và
* Mọi cơ chế ủy quyền từ chối truy cập đối với các đối tượng đã xác thực với quyền truy cập không phù hợp và đối với các đối tượng chưa xác thực.

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

**3.5.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

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

**b) Phương pháp đánh giá**

i. Áp dụng tất cả các Phương pháp đánh giá được nêu trong Kịch bản kiểm thử 3.5-4-2 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 bảo mật 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.

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

ii. Đánh giá chức năng liệu các cơ chế giao tiếp 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 giao tiếp dựa trên mạng.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Đối tượng chưa được xác thực, đối tượng có danh tính 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; và
* Đối tượng đã được xác thực với quyền truy cập thích hợp có thể truy cập chức năng của thiết bị; và
* Không có dấu hiệu nào cho thấy cơ chế bảo vệ xác thực khác với tài liệu **IXIT**; và
* Mọi cơ chế giao tiếp dựa trên mạng được phát hiện đều được tài liệu hóa trong **IXIT**.

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

### 3.5.3. Nhóm kiểm thử 2.5-3

**3.5.3.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5-3, điều 2.5 Quy chuẩn này.

**3.5.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc thông số bảo mật bí mật khi truyền qua môi trường mạng sử dụng kênh giao tiếp an toàn.

**b) Phương pháp đánh giá**

Đối với tất cả các “Cơ chế kết nối” có thể truy cập từ xa theo "Mô tả" trong **IXIT 11-ComMech** được tham chiếu trong bất kỳ tham số bảo mật quan trọng nào trong **IXIT 10-SecParam**, áp dụng tất cả các phương pháp đánh giá như đã chỉ định trong Kịch bản kiểm thử 3.5-1-1 với giới hạn rằng ít nhất là đảm bảo bảo mật về tính bảo mật cần được đáp ứng.

**c) Kết luận đánh giá**

i. **Đáp ứng:** được đưa ra nếu đối với tất cả các cơ chế giao tiếp được sử dụng để giao tiếp các tham số bảo mật quan trọng qua các giao diện mạng có thể truy cập từ xa:

* Các đảm bảo bảo mật là phù hợp cho trường hợp sử dụng giao tiếp an toàn; và
* Cơ chế phù hợp để đạt được các đảm bảo bảo mật đối với trường hợp sử dụng; và
* Tất cả các chi tiết mật mã được sử dụng được coi là thực hành tốt nhất cho trường hợp sử dụng; và
* Tất cả các chi tiết mật mã được sử dụng không được biết là dễ bị tấn công khả thi.

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

**3.5.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của mật mã được sử dụng để giao tiếp các tham số bảo mật quan trọng qua các giao diện mạng có thể truy cập từ xa.

**b) Phương pháp đánh giá**

Đối với tất cả các "Cơ chế Giao tiếp" có thể truy cập từ xa theo "Mô tả" trong **IXIT 11-ComMech** được tham chiếu trong bất kỳ tham số bảo mật quan trọng nào trong **IXIT 10-SecParam**, áp dụng tất cả các phương pháp đánh giá như đã chỉ định trong Kịch bản kiểm thử 3.5-1-2.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm: Không có dấu hiệu nào cho thấy bất kỳ cài đặt mật mã nào được sử dụng khác với tài liệu IXIT của nó.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.5.4. Nhóm kiểm thử 2.5-4

**3.5.4.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.5-4, điều 2.5 Quy chuẩn này.

**3.5.4.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc nhà sản xuất công bố và tuân thủ quy trình quản lý các thông số bảo mật bí mật được sử dụng bởi thiết bị camera.

**b) Phương pháp đánh giá**

i. Đánh giá liệu quy trình quản lý an toàn của các tham số bảo mật quan trọng có bao phủ toàn bộ vòng đời của một tham số bảo mật quan trọng, bao gồm:

* Tạo ra; và
* Cung cấp; và
* Lưu trữ; và
* Cập nhật; và
* Ngừng hoạt động, lưu trữ và hủy bỏ; và
* Các quy trình xử lý việc hết hạn và bị xâm phạm; theo các quy trình trong **IXIT 14-SecMgmt**.

ii. Kiểm tra xem "Xác nhận quản lý bảo mật" trong **IXIT 4-Conf** có được xác nhận.

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Quản lý an toàn bao phủ toàn bộ vòng đời của một tham số bảo mật quan trọng theo các quy trình của nó; và
* Có một sự xác nhận cho việc thực hiện.

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

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

### 3.6.1. Nhóm kiểm thử 2.6-1

**3.6.1.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6-1, điều 2.6 Quy chuẩn này.

**3.6.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc tất cả các giao diện mạng và logic không sử dụng phải được vô hiệu hóa.

**b) Phương pháp đánh giá**

Đối với mỗi giao diện mạng và logic trong **IXIT 15-Intf** được mô tả là đang hoạt động theo "Trạng thái", đánh giá xem mục đích của giao diện trong "Mô tả" có cung cấp sự biện minh hợp lệ cho việc được kích hoạt hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

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

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.6.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các giao diện mạng và logic của thiết bị camera và tính đầy đủ của tài liệu IXIT.

**b) Phương pháp đánh giá**

i. Đối với mỗi giao diện mạng và logic trong **IXIT 15-Intf**, kiểm thử chức năng của sản phẩm được đánh giá xem trạng thái của giao diện có khớp với "Trạng thái" trong tài liệu IXIT hay không.

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

ii. Đánh giá chức năng xem các giao diện mạng hoặc logic không được ghi chép trong **IXIT 15-Intf** có khả dụng qua một giao diện mạng trên thiết bị camera hay không.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Mỗi giao diện mạng hoặc logic được ghi chép mà được đánh dấu là vô hiệu trong tài liệu **IXIT** được xác nhận là vô hiệu hoặc không thể truy cập trên Thiết bị camera; và
* Mỗi giao diện mạng và logic được phát hiện đều được ghi chép trong tài liệu **IXIT**.

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

### 3.6.2. Nhóm kiểm thử 2.6-2

**3.6.2.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6-2, điều 2.6 Quy chuẩn này.

**3.6.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc ở trạng thái hoạt động ban đầu, khi người sử dụng chưa được xác thực, tất cả các giao diện quản trị của thiết bị không cung cấp thông tin liên quan đến thông số bảo mật bí mật và thông số bảo mật nhạy cảm của camera.

**b) Phương pháp đánh giá**

i. Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, đánh giá xem thông tin "Thông tin có thể tiết lộ" được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo và được chỉ ra là không liên quan đến bảo mật có thực sự liên quan đến bảo mật hay không.

ii. Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, đánh giá xem thông tin "Thông tin có thể tiết lộ" được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo và được chỉ ra là liên quan đến bảo mật có cần thiết cho hoạt động của thiết bị camera hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ được đưa ra nếu đối với mọi giao diện mạng:

* Mọi thông tin liên quan đến bảo mật được tiết lộ bởi giao diện mà không cần xác thực trong trạng thái khởi tạo đều được ghi nhận là như vậy; và
* Mọi thông tin liên quan đến bảo mật 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.

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

**3.6.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của thông tin được tiết lộ bởi các giao diện mạng mà không cần xác thực trong trạng thái khởi tạo.

**b) Phương pháp đánh giá**

Đối với mỗi giao diện mạng trong **IXIT 15-Intf**, kiểm thử chức năng của sản phẩm được đánh giá xem liệu có thể quan sát thông tin liên quan đến bảo mật từ giao diện mà không cần xác thực trong trạng thái khởi tạo và không được mô tả trong "Thông tin có thể tiết lộ".

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

Đối với mọi giao diện mạng, chỉ có thể quan sát được thông tin liên quan đến bảo mật đã được mô tả trong tài liệu IXIT.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.6.3. Nhóm kiểm thử 2.6-3

**3.6.3.0. Mục tiêu kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.6-3, điều 2.6 Quy chuẩn này.

**3.6.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng vô hiệu hóa giao diện gỡ lỗi có thể truy cập vật lý, bằng phần mềm.

**b) Phương pháp đánh giá**

i. Đối với mỗi giao diện vật lý trong **IXIT 15-Intf** được mô tả là giao diện gỡ lỗi có thể truy cập theo "Giao diện gỡ lỗi", đánh giá xem liệu các phương tiện bảo vệ cho giao diện trong “Phương pháp bảo vệ” có bao gồm cơ chế phần mềm để vô hiệu hóa giao diện hay không.

ii. Đối với mỗi giao diện vật lý trong **IXIT 15-Intf** được mô tả là giao diện gỡ lỗi có thể truy cập nhưng không được chỉ ra là yêu cầu tạm thời theo “Mô tả”, kiểm tra xem giao diện có bị vô hiệu hóa vĩnh viễn theo “Trạng thái” hay không.

iii. Đối với mỗi giao diện vật lý trong IXIT 15-Intf được mô tả là giao diện gỡ lỗi có thể truy cập và được chỉ ra là yêu cầu tạm thời theo “Mô tả”, kiểm tra xem giao diện có bị vô hiệu hóa theo mặc định theo “Trạng thái” hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** sẽ tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Đối với mọi giao diện gỡ lỗi vật lý có thể truy cập, có một cơ chế phần mềm được mô tả để vô hiệu hóa giao diện; và
* Đối với mọi giao diện gỡ lỗi vật lý có thể truy cập mà không được chỉ ra là yêu cầu tạm thời, giao diện bị vô hiệu hóa vĩnh viễn; và
* Đối với mọi giao diện gỡ lỗi vật lý có thể truy cập được chỉ ra là yêu cầu tạm thời, giao diện bị vô hiệu hóa theo mặc định.

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

**3.6.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các giao diện gỡ lỗi vật lý có thể truy cập của Thiết bị camera và tính đầy đủ của tài liệu IXIT.

**b) Phương pháp đánh giá**

i. Đối với mỗi giao diện vật lý có thể truy cập trên Thiết bị camera được chỉ ra là "Giao diện gỡ lỗi" trong **IXIT 15-Intf**, kiểm thử chức năng của sản phẩm được đánh giá xem liệu giao diện có bị vô hiệu hóa hay không.

**CHÚ THÍCH 1:** Đối với Phương pháp đánh giá này, đảm bảo rằng giao diện ở trạng thái mặc định của nó.

ii. Đối với mỗi giao diện vật lý có thể truy cập trên thiết bị camera, đánh giá chức năng xem liệu giao diện có thể được sử dụng cho mục đích gỡ lỗi mặc dù nó không được chỉ ra là "Giao diện gỡ lỗi" trong **IXIT 15-Intf** hay không.

**CHÚ THÍCH 2:** Đối với Phương pháp đánh giá này, có thể thử sử dụng giao diện như một giao diện gỡ lỗi bằng cách sử dụng các phương pháp và công cụ tiêu chuẩn.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Mọi giao diện gỡ lỗi vật lý có thể truy cập đều bị vô hiệu hóa; và
* Mọi giao diện gỡ lỗi vật lý đều được chỉ ra như vậy trong tài liệu IXIT.

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

## 3.7. Bảo vệ dữ liệu người sử dụng

### 3.7.1. Nhóm kiểm thử 2.7-1

**3.7.1.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.7-1, điều 2.7 Quy chuẩn này.

**3.7.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc dữ liệu cá nhân thu thập, xử lý bởi thiết bị camera được truyền giữa thiết bị và các dịch vụ liên quan phải sử dụng kênh kết nối được mã hóa an toàn.

**b) Phương pháp đánh giá**

Đối với tất cả "Cơ chế kết nối" trong **IXIT 11-ComMech** được tham chiếu trong bất kỳ dữ liệu cá nhân nhạy cảm nào trong **IXIT** **21-PersData** theo “Tính nhạy cảm”, nơi đối tác giao tiếp là một dịch vụ liên quan, áp dụng tất cả các Phương pháp đánh giá như được chỉ định trong Kịch bản kiểm thử 3.5-1-1 với giới hạn là phải đảm bảo ít nhất là bảo mật.

**CHÚ THÍCH:** Trong trường hợp này, đảm bảo an ninh "bảo mật" có nghĩa là bảo vệ sự bảo mật trước các bên không được phép. Điều này có thể bao gồm xác thực đối tác giao tiếp.

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với tất cả các cơ chế giao tiếp được sử dụng để giao tiếp dữ liệu cá nhân nhạy cảm giữa thiết bị và dịch vụ liên quan:

* Các đảm bảo an ninh phù hợp cho trường hợp sử dụng trong giao tiếp dữ liệu cá nhân nhạy cảm giữa thiết bị và dịch vụ liên quan; và
* Cơ chế phù hợp để đạt được các đảm bảo an ninh liên quan đến trường hợp sử dụng; và
* Tất cả các chi tiết mã hóa đã sử dụng được coi là phương pháp tốt nhất cho trường hợp sử dụng; và
* Tất cả các chi tiết mã hóa đã sử dụng không được biết là dễ bị tấn công.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.7.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của mã hóa được sử dụng để giao tiếp dữ liệu cá nhân nhạy cảm giữa thiết bị và các dịch vụ liên quan.

**b) Phương pháp đánh giá**

Đối với tất cả "Cơ chế kết nối" trong IXIT 11-ComMech được tham chiếu trong bất kỳ dữ liệu cá nhân nhạy cảm nào trong IXIT 21-PersData theo “Tính nhạy cảm”, nơi đối tác giao tiếp là một dịch vụ liên quan, áp dụng tất cả các Phương pháp đánh giá như được chỉ định trong Kịch bản kiểm thử 3.5-1-2.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng, bao gồm:

Không có dấu hiệu nào cho thấy bất kỳ cài đặt mã hóa nào được sử dụng khác với tài liệu IXIT của nó.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.7.2. Nhóm kiểm thử 2.7-2

**3.7.2.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.7-2, điều 2.7 Quy chuẩn này.

**3.7.2.1. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc tất cả các chức năng cảm biến của camera được mô tả trong tài liệu đặc tả kỹ thuật.

**b) Phương pháp đánh giá**

i. Kiểm thử chức năng của sản phẩm được đánh giá liệu tài liệu về các khả năng cảm biến bên ngoài có thể truy cập được như đã ghi trong “Tài liệu mô tả về các cảm biến camera sử dụng” trong **IXIT 2-UserInfo**.

ii. Đánh giá liệu tài liệu về các khả năng cảm biến bên ngoài như đã ghi trong “Tài liệu mô tả về các cảm biến camera sử dụng” trong **IXIT 2-UserInfo** có dễ hiểu đối với người dùng có kiến thức kỹ thuật hạn chế hay không (xem Phụ lục D).

iii. Đánh giá liệu tất cả các khả năng cảm biến rõ ràng của Thiết bị camera có được ghi lại trong **IXIT 22-ExtSens** hay không.

**CHÚ THÍCH:** Đánh giá này có thể bao gồm kiểm tra trực quan vỏ Thiết bị camera để xác định các dấu hiệu của các khả năng cảm biến chưa được ghi lại. Nếu phát hiện có dấu hiệu, việc mở vỏ có thể cung cấp sự rõ ràng.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Tài liệu có thể truy cập được theo IXIT; và
* Tài liệu dễ hiểu đối với người dùng có kiến thức kỹ thuật hạn chế; và
* Mỗi khả năng cảm biến rõ ràng của Thiết bị camera đều được ghi lại cho người dùng.

ii. **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 2.8-1

**3.8.1.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8-1, điều 2.8 Quy chuẩn này.

**3.8.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng cho phép khôi phục lại hoạt động bình thường khi xảy ra sự cố mất điện hoặc mất kết nối mạng.

**b) Phương pháp đánh giá**

i. Đánh giá liệu sự kết hợp của các cơ chế chống chịu trong **IXIT 23-ResMech** có phù hợp để bảo vệ chống lại sự cố mạng và mất điện theo “Điều kiện bảo đảm bảo mật” hay không.

ii. Đối với mỗi cơ chế chống chịu trong **IXIT 23-ResMech**, đánh giá liệu cơ chế đó theo “Mô tả” có phù hợp để đạt được “Điều kiện bảo đảm bảo mật” hay không.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Các cơ chế chống chịu phù hợp để bảo vệ chống lại sự cố mạng và mất điện; và
* Mỗi cơ chế chống chịu phù hợp để đạt được các đảm bảo an ninh.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.8.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các cơ chế chống chịu với sự cố mạng và mất điện.

**b) Phương pháp đánh giá**

i. Ngắt kết nối mạng của Thiết bị camera và đánh giá chức năng liệu các cơ chế chống chịu hoạt động như đã mô tả trong **IXIT 23-ResMech**.

ii. Ngắt nguồn cung cấp điện của Thiết bị camera và đánh giá chức năng liệu các cơ chế chống chịu hoạt động như đã mô tả trong **IXIT 23-ResMech**.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng:

Không có dấu hiệu cho thấy hoạt động của các cơ chế chống chịu trong quá trình mất kết nối mạng và mất điện khác với tài liệu IXIT của nó.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.8.2. Nhóm kiểm thử 2.8-2

**3.8.2.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8-2, điều 2.8 Quy chuẩn này.

**3.8.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera hoạt động bình thường đối với các chức năng nội bộ khi bị mất kết nối mạng và khôi phục hoạt động bình thường khi kết nối mạng được khôi phục.

**b) Phương pháp đánh giá**

i. Áp dụng tất cả các Phương pháp đánh giá như đã nêu trong Kịch bản kiểm thử 3.9-1-1 cho các cơ chế chống chịu trong **IXIT** **23-ResMech**.

ii. Đánh giá liệu các cơ chế chống chịu trong **IXIT 23-ResMech** bảo vệ chống lại sự cố kết nối mạng theo "Loại" có phù hợp để đảm bảo rằng Thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ trong trường hợp mất kết nối mạng.

iii. Đánh giá liệu các cơ chế chống chịu trong **IXIT 23-ResMech** bảo vệ chống lại sự cố mất điện theo "Loại" có phù hợp để đảm bảo rằng Thiết bị camera khôi phục kết nối và chức năng sau khi mất điện trong trạng thái tương tự hoặc được cải thiện so với trước đó.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Các cơ chế chống chịu phù hợp để bảo vệ chống lại sự cố kết nối mạng và mất điện; và
* Mỗi cơ chế chống chịu phù hợp để đạt được các đảm bảo an ninh của nó; và
* Các cơ chế chống chịu phù hợp để đảm bảo rằng Thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ trong trường hợp mất kết nối mạng; và
* Các cơ chế chống chịu phù hợp để đảm bảo rằng Thiết bị camera khôi phục sạch sẽ sau khi mất điện.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.8.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các cơ chế chống chịu với sự cố mạng và mất điện, hoạt động trong quá trình mất kết nối mạng và phục hồi sau khi mất điện.

**b) Phương pháp đánh giá**

i. Thử nghiệm ngắt kết nối mạng của Thiết bị camera và đánh giá chức năng liệu các cơ chế chống chịu hoạt động như đã mô tả trong **IXIT 23-ResMech** và thiết bị camera vẫn hoạt động và có thể hoạt động cục bộ sau khi mất kết nối mạng.

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

ii. Thử nghiệm ngắt nguồn cung cấp điện của thiết bị camera và đánh giá chức năng liệu các cơ chế chống chịu hoạt động như đã mô tả trong **IXIT 23-ResMech** và 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.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Không có dấu hiệu cho thấy hoạt động của các cơ chế chống chịu trong quá trình mất kết nối mạng hoặc mất điện khác với tài liệu IXIT của nó; và
* Không có dấu hiệu cho thấy Thiết bị camera không tiếp tục hoạt động và có thể hoạt động cục bộ sau khi mất kết nối mạng; và
* Không có dấu hiệu cho thấy Thiết bị camera không khôi phục kết nối và chức năng sau khi mất điện trong trạng thái tương tự hoặc được cải thiện so với trước đó.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

### 3.8.3. Nhóm kiểm thử 2.8-3

**3.8.3.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.8-3, điều 2.8 Quy chuẩn này.

**3.8.3.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc khi thiết bị camera khôi phục kết nối mạng, việc khôi phục lại kết nối từ camera đến các dịch vụ liên kết được thực hiện tuần tự, tránh xung đột mạng.

**b) Phương pháp đánh giá**

i. Đối với mỗi cơ chế kết nối trong **IXIT 11-ComMech**, đánh giá liệu "Biện pháp khôi phục" có phù hợp để đạt được kết nối với mạng một cách có trật tự, đồng thời xem xét khả năng của hạ tầng.

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

ii. Đối với mỗi cơ chế truyền thông trong **IXIT 11-ComMech**, đánh giá liệu "Biện pháp khôi phục" có phù hợp để hỗ trợ hoạt động của một mạng ổn định, đồng thời xem xét khả năng của hạ tầng.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* mỗi cơ chế truyền thông cung cấp các biện pháp phù hợp để đạt được kết nối với mạng một cách có trật tự; và
* mỗi cơ chế truyền thông cung cấp các biện pháp phù hợp để hỗ trợ hoạt động của một mạng ổn định.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.8.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng các biện pháp chống chịu cho các cơ chế truyền thông.

**b) Phương pháp đánh giá**

Đánh giá chức năng liệu các “Biện pháp khôi phục” đã được triển khai cho mỗi “Cơ chế kết nối” trong **IXIT 11-ComMech** được thực hiện đúng như mô tả, đặc biệt là xem xét việc bảo vệ chống lại việc kết nối lại hàng loạt đồng thời.

**Ví dụ:** Nếu Thiết bị camera sử dụng giao thức TCP/IP, sử dụng công cụ giám sát mạng để xác minh quá trình khởi tạo và kết thúc liên quan đến thiết lập kết nối tuân theo các tiêu chuẩn tương ứng có thể giúp thu thập chỉ dẫn.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng:

Không có dấu hiệu cho thấy hoạt động của bất kỳ biện pháp chống chịu nào đã triển khai khác với tài liệu IXIT của nó.

ii. **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 2.9-1

**3.9.1.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.9-1, điều 2.9 Quy chuẩn này.

**3.9.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng cho phép người sử dụng xóa dữ liệu cá nhân và cấu hình hệ thống được thu thập và lưu trữ trên thiết bị camera.

**b) Phương pháp đánh giá**

i. Đánh giá liệu ít nhất một chức năng được cung cấp theo **IXIT 25-DelFunc**, mà người dùng có thể thực hiện với kiến thức kỹ thuật hạn chế (xem Phụ lục D) theo "Mô tả" và "Khởi động và tương tác" để xóa dữ liệu người dùng khỏi thiết bị theo "Đối tượng".

ii. Đánh giá liệu mỗi chức năng trong **IXIT 25-DelFunc** có đủ khả năng xóa dữ liệu người dùng được nhắm đến từ thiết bị.

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

iii. Đánh giá liệu các chức năng để xóa dữ liệu người dùng trong **IXIT 25-DelFunc** có bao gồm dữ liệu cá nhân, cấu hình người dùng và các vật liệu mã hóa liên quan đến người dùng.

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

**CHÚ THÍCH 3**: Vật liệu mã hóa có thể là mật khẩu người dùng hoặc khóa.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu không có dữ liệu người dùng nào được lưu trữ trên thiết bị; hoặc nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* ít nhất một chức năng đơn giản để xóa dữ liệu người dùng khỏi thiết bị được cung cấp cho người dùng; và
* chức năng được mô tả đủ khả năng xóa dữ liệu người dùng được nhắm đến từ thiết bị; và
* dữ liệu cá nhân, cấu hình người dùng và vật liệu mã hóa được bao gồm trong các chức năng để xóa dữ liệu người dùng khỏi thiết bị.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.9.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các chức năng xóa dữ liệu người dùng của Thiết bị camera.

**b) Phương pháp đánh giá**

i. Tạo dữ liệu người dùng điển hình trên Thiết bị camera liên quan đến việc sử dụng thiết bị.

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

ii. Thực hiện mỗi chức năng để xóa dữ liệu người dùng khỏi thiết bị theo "Đối tượng" trong **IXIT 25-DelFunc** và đánh giá chức năng xem "Khởi tạo và tương tác" có phù hợp với IXIT không.

iii. Thực hiện mỗi chức năng để xóa dữ liệu người dùng khỏi thiết bị theo "Đối tượng" trong **IXIT 25-DelFunc** và đánh giá chức năng xem liệu dữ liệu người dùng liên quan có còn tồn tại sau khi hoàn thành thao tác không.

**VÍ DỤ**: Việc so sánh giữa cấu hình trước và sau khi xóa có thể hữu ích để thu thập thông tin liên quan đến dữ liệu người dùng chưa được xóa.

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với bất kỳ chức năng nào để xóa dữ liệu người dùng khỏi thiết bị:

* việc khởi động và tương tác của người dùng phù hợp với IXIT; và
* không có dấu hiệu nào cho thấy dữ liệu người dùng liên quan không được xóa thành công.

ii. **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 2.10-1

**3.10.1.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.10-1, điều 2.10 Quy chuẩn này.

**3.10.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera phải kiểm tra tính hợp lệ của dữ liệu đầu vào trước khi xử lý, thông qua các giao diện người sử dụng, giao diện lập trình ứng dụng (APIs) hoặc giữa các dịch vụ liên kết và thiết bị.

**b) Phương pháp đánh giá**

i. Đánh giá liệu tổ hợp các phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal** có bao gồm tất cả các nguồn dữ liệu đầu vào bao gồm:

* các giao diện người dùng, cho phép đầu vào từ người dùng trong **IXIT 27-UserIntf**; và
* các giao diện lập trình ứng dụng (APIs), cho phép đầu vào từ các nguồn bên ngoài trong **IXIT 28-ExtAPI**; và
* các giao tiếp mạng, cho phép đầu vào dữ liệu theo các phương pháp giao tiếp truy cập từ xa tương ứng trong **IXIT 11-ComMech**.

ii. Đối với mỗi phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal**, đánh giá liệu nó có hiệu quả trong việc xác thực dữ liệu đầu vào tương ứng hay không.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* các phương pháp xác thực dữ liệu đầu vào bao gồm dữ liệu đầu vào qua giao diện người dùng, truyền qua APIs và giữa các mạng trong các dịch vụ và thiết bị; và
* mọi phương pháp xác thực dữ liệu đầu vào được mô tả đều hiệu quả trong việc xác thực dữ liệu đầu vào tương ứng.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.10.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của các phương pháp xác thực dữ liệu đầu vào của thiết bị camera và sự hoàn thiện của tài liệu IXIT.

**b) Phương pháp đánh giá**

i. Đánh giá chức năng liệu mỗi phương pháp xác thực dữ liệu đầu vào trong **IXIT 29-InpVal** có ngăn chặn được việc xử lý dữ liệu đầu vào không mong muốn hay không.

**CHÚ THÍCH 1:** Có thể tự do lựa chọn một nguồn dữ liệu đầu vào cho mỗi phương pháp xác thực dữ liệu đầu vào.

**CHÚ THÍCH 2:** Thử nghiệm tất cả các thông tin xác thực của một người dùng để cố gắng lạm dụng.

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

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

Ví dụ 2: Nếu thiết bị camera có giao diện web, việc sử dụng công cụ quét ứng dụng web để xác minh rằng không có các vấn đề liên quan đến web như XSS, SQL injection, hoặc CSRF có thể hữu ích để thu thập các chỉ số.

ii. Đánh giá chức năng liệu tất cả các giao diện người dùng của thiết bị camera có được mô tả trong **IXIT 27-UserIntf** theo tài liệu dành cho người dùng, ví dụ hướng dẫn sử dụng.

iii. Đánh giá chức năng liệu tất cả các API truy cập từ xa của Thiết bị camera có được mô tả trong **IXIT 28-ExtAPI**.

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

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* Phương pháp xác thực dữ liệu đầu vào bảo vệ được việc xử lý dữ liệu đầu vào không mong muốn; và
* mọi giao diện người dùng được phát hiện đều được ghi trong IXIT; và
* mọi API truy cập từ xa được phát hiện đều được ghi trong IXIT.

ii. **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 2.11-1

**3.11.1.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11-1, điều 2.11 Quy chuẩn này.

**3.11.1.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc nhà sản xuất cung cấp đầy đủ thông tin về mục đích, các 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).

**b) Phương pháp đánh giá**

Đánh giá liệu "Tài liệu về dữ liệu cá nhân" trong **IXIT 2-UserInfo** có phù hợp để người tiêu dùng thu thập thông tin về việc xử lý dữ liệu cá nhân.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng:

Thông tin về việc xử lý dữ liệu cá nhân được cung cấp một cách phù hợp cho người tiêu dùng.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.11.1.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của thông tin người dùng liên quan đến việc xử lý dữ liệu cá nhân.

**b) Phương pháp đánh giá**

i. Đánh giá chức năng liệu thông tin cung cấp về việc xử lý dữ liệu cá nhân (thông tin đã thu thập) có nhất quán với mô tả trong "Tài liệu về dữ liệu cá nhân" trong **IXIT 2-UserInfo**.

ii. Đánh giá chức năng liệu thông tin đã 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 khớp với mô tả trong "Biện pháp xử lý" trong **IXIT 21-PersData**.

iii. Đánh giá chức năng liệu thông tin đã thu thập mô tả dữ liệu cá nhân nào đang được xử lý một cách dễ hiểu đối với người dùng có kiến thức kỹ thuật hạn chế (xem Phụ lục D).

iv. Đánh giá chức năng liệu thông tin đã thu thập mô tả cách thức dữ liệu cá nhân đang được sử dụng, bởi ai, và cho mục đích gì một cách dễ hiểu đối với người dùng có kiến thức kỹ thuật hạn chế (xem Phụ lục D).

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* thông tin về việc xử lý dữ liệu cá nhân có thể được thu thập như mô tả; và
* thông tin đã thu thập về việc xử lý dữ liệu cá nhân khớp với mô tả của chúng; và
* dữ liệu cá nhân đang được xử lý được mô tả rõ ràng và minh bạch; và
* cách thức dữ liệu cá nhân đang được sử dụng, bởi ai, và cho mục đích gì được mô tả rõ ràng và minh bạch.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

### 3.11.2. Nhóm kiểm thử 2.11-2

**3.11.2.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11-2, điều 2.11 Quy chuẩn này.

**3.11.2.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng cho phép xác nhận việc đồng ý của người sử dụng đối với việc cho phép camera thu thập và xử lý dữ liệu cá nhân.

**b) Phương pháp đánh giá**

Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở sự đồng ý của người tiêu dùng theo "Thu thập sự đồng ý", đánh giá liệu lựa chọn đồng ý cho nhà cung cấp thu thập thông tin:

* có được đưa ra một cách tự do; và
* có được đưa ra một cách rõ ràng; và
* có được đưa ra một cách rõ ràng theo mô tả của "Thu thập sự đồng ý".

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở sự đồng ý của người tiêu dùng:

* có mô tả về cách thức để thể hiện sự đồng ý (lựa chọn đồng ý cho nhà cung cấp thu thập thông tin) đối với việc xử lý dữ liệu cá nhân cho các mục đích cụ thể; và
* lựa chọn đồng ý cho nhà cung cấp thu thập thông tin được đưa ra một cách tự do, rõ ràng và rõ ràng.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

**3.11.2.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của Kịch bản kiểm thử này là đánh giá chức năng của sự đồng ý của người tiêu dùng đối với việc xử lý dữ liệu cá nhân.

**b) Phương pháp đánh giá**

Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý trên cơ sở sự đồng ý của người tiêu dùng theo "Thu thập sự đồng ý", đánh giá chức năng liệu sự đồng ý của người tiêu dùng đối với việc xử lý dữ liệu cá nhân có được thu thập như mô tả trong IXIT.

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với mỗi loại dữ liệu cá nhân được xử lý trên cơ sở sự đồng ý của người tiêu dùng:

Cách thức thu thập sự đồng ý của người tiêu dùng phù hợp với mô tả.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.11.3. Nhóm kiểm thử 2.11-3

**3.11.3.0. Mục tiêu nhóm kiểm thử**
Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11-3, điều 2.11 Quy chuẩn này.

**3.11.3.1. Đánh giá tài liệu kiểm thử**
**a) Mục đích kiểm thử**Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera có chức năng cho phép xác nhận việc hủy đồng ý của người sử dụng về về việc cho phép camera thu thập và xử lý dữ liệu cá nhân.

**b) Phương pháp đánh giá**

Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý dựa trên sự đồng ý của người tiêu dùng theo "Thu thập sự đồng ý", đánh giá liệu thông tin về "Rút lại sự đồng ý" có mô tả cách rút lại sự đồng ý đối với việc xử lý dữ liệu cá nhân vào bất cứ lúc nào bằng cách cấu hình thiết bị IoT và chức năng dịch vụ một cách thích hợp.

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với mỗi loại dữ liệu cá nhân được xử lý dựa trên sự đồng ý của người tiêu dùng:

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

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.11.3.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của tình huống kiểm thử này là đánh giá chức năng của việc rút lại sự đồng ý của người tiêu dùng đối với việc xử lý dữ liệu cá nhân.

**b) Phương pháp đánh giá**

Đối với mỗi dữ liệu cá nhân trong **IXIT 21-PersData** được xử lý dựa trên sự đồng ý của người tiêu dùng theo "Thu thập sự đồng ý", kiểm thử chức năng của sản phẩm được đánh giá xem liệu sự đồng ý của người tiêu dùng đối với việc xử lý dữ liệu cá nhân có thể được rút lại như mô tả trong "Rút lại sự đồng ý".

**c) Kết luận đánh giá**

i. **Đáp ứng:** đối với mỗi loại dữ liệu cá nhân được xử lý dựa trên sự đồng ý của người tiêu dùng:

Cách thức rút lại sự đồng ý của người tiêu dùng phù hợp với mô tả.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

### 3.11.4. Nhóm kiểm thử 2.11-4

**3.11.4.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11-4, điều 2.11 Quy chuẩn này.

**3.11.4.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc dữ liệu đo đạc từ xa trên thiết bị camera được thu thập bởi nhà sản xuất (nếu có) phải được mô tả đầy đủ về mục đích, đối tượng thu thập và nơi lưu trữ.

**b) Phương pháp đánh giá**

Đánh giá liệu "Tài liệu về dữ liệu đo đạc từ xa" trong **IXIT 2-UserInfo** có phù hợp để người tiêu dùng có thể nhận được thông tin về việc xử lý dữ liệu đo đạc từ xa.

**c) Kết luận đánh giá**

i. **Đáp ứng:** nếu yêu cầu dưới đây được đáp ứng:

Thông tin về việc xử lý dữ liệu đo đạc từ xa được cung cấp một cách phù hợp cho người tiêu dùng.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.11.4.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Mục đích của tình huống kiểm thử này là đánh giá chức năng của thông tin cho người dùng về việc xử lý dữ liệu đo đạc từ xa.

**b) Phương pháp đánh giá**

i. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thông tin cung cấp về việc xử lý dữ liệu đo đạc từ xa (thông tin thu được) có nhất quán với mô tả trong "Tài liệu về dữ liệu đo đạc từ xa" của **IXIT 2-UserInfo**.

ii. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thông tin thu được về việc xử lý dữ liệu đo đạc từ xa truy cập từ "Tài liệu về dữ liệu đo đạc từ xa" trong **IXIT 2-UserInfo** có khớp với "Mục đích" được mô tả trong **IXIT 24-TelData**.

iii. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thông tin thu được có mô tả dữ liệu đo đạc từ xa nào đang được thu thập hay không.

iv. Kiểm thử chức năng của sản phẩm được đánh giá xem liệu thông tin thu được có mô tả rõ ràng cách dữ liệu đo đạc từ xa được sử dụng, bởi ai và cho mục đích gì.

**c) Kết luận đánh giá**
i. **Đáp ứng:** nếu tất cả các các yêu cầu dưới đây được đáp ứng, bao gồm:

* thông tin về việc xử lý dữ liệu đo đạc từ xa có thể được thu thập như mô tả; và
* thông tin thu được về việc xử lý dữ liệu đo đạc từ xa khớp với mô tả của chúng; và
* dữ liệu đo đạc từ xa đang được thu thập được mô tả; và
* cách dữ liệu đo đạc từ xa được sử dụng, bởi ai và cho mục đích gì được mô tả đầy đủ.

ii. **Không đáp ứng:** nếu một trong các yêu cầu trên không đáp ứng.

### 3.11.5. Nhóm kiểm thử 2.11-5

**3.11.5.0. Mục tiêu nhóm kiểm thử**

Kiểm thử thiết bị camera đáp ứng hay không yêu cầu 2.11-5, điều 2.11 Quy chuẩn này.

**3.11.5.1. Đánh giá tài liệu kiểm thử**

**a) Mục đích kiểm thử**

Đánh giá tài liệu kiểm thử mô tả đầy đủ các thông tin để minh chứng việc camera và các dịch vụ liên kết có tính năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

**b) Phương pháp đánh giá**

Đối với dữ liệu cá nhân trong **IXIT 21-PersData** đánh giá xem camera và các dịch vụ liên kết có tính năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam đối với loại dữ liệu này.

**c) Kết luận đánh giá**

i. **Đáp ứng:** Tài liệu kiểm thử mô tả đầy đủ thông tin để minh chứng camera và các dịch vụ liên kết có tính năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

ii. **Không đáp ứng:** Nếu không đáp ứng yêu cầu trên.

**3.11.5.2. Kiểm thử chức năng của sản phẩm được đánh giá**

**a) Mục đích kiểm thử**

Kiểm chứng bằng thực nghiệm việc camera và các dịch vụ liên kết có chức năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

**b) Phương pháp đánh giá**

Đánh giá bằng thực nghiệm để minh chứng camera và các dịch vụ liên kết có chức năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

**c) Kết luận đánh giá**
i. **Đáp ứng:** Đánh giá bằng thực nghiệm chứng minh được camera và các dịch vụ liên kết có chức năng cho phép thiết lập cấu hình để camera và các dịch vụ liên kết xử lý, lưu trữ và khai thác dữ liệu tại Việt Nam.

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

4. QUY ĐỊNH VỀ QUẢN LÝ

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

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

5. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

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

6. TỔ CHỨC THỰC HIỆN

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

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

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

PHỤ LỤC A

**(Quy định)**

**DANH MỤC THÔNG TIN PHỤC VỤ ĐÁNH GIÁ**

**IXIT 1-AuthMech: Cơ chế xác thực**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phương thức xác thực trong bảng IXIT 1-AuthMech. Ví dụ: AuthMech-1, AuthMech-2,... |
| **Mô tả** | Mô tả ngắn gọn về cơ chế xác thực và các bước xử lý cơ bản. Mô tả mục đích của phương thức xác thực được sử dụng. Ví dụ: phương thức xác thực người sử dụng qua giao thức HTTPS, xác thực qua giao diện lập trình API qua giao thức SOAP. |
| **Giá trị xác thực** | Mô tả về Giá trị xác thực được sử dụng. Ví dụ: username, password hoặc secret key. |
| **Cơ chế khởi tạo mật khẩu** | Mô tả Cơ chế Khởi tạo Giá trị xác thực đáp ứng các yêu cầu an toàn theo quy định. |
| **Điều kiện đảm bảo bảo mật** | Mô tả các yếu tố cần thực hiện để phương thức xác thực được bảo đảm thực hiện đúng chức năng như thiết kế. |
| **Phương thức mã hóa** | Mô tả phương thức mã hóa mà mỗi phương thức xác thực sử dụng. |
| **Ngăn chặn tấn công vét cạn** | Mô tả phương pháp ngăn chặn tấn công tấn công vét cạn qua các giao diện mạng. |

**IXIT 2-UserInfo: Thông tin cung cấp cho người dùng**

|  |  |
| --- | --- |
| **Tài liệu hướng dẫn thay đổi thông tin xác thực** | Tài liệu hướng dẫn cho người dùng cách thức thay đổi giá trị xác thực. |
| **Tài liệu hướng dẫn bảo trì thiết bị** | Tài liệu hướng dẫn cho người dùng cách thức bảo trì thiết bị camera. |
| **Tài liệu mô tả về các cảm biến camera sử dụng** | Tài liệu mô tả về các thông tin, dữ liệu được thu thập bở các cảm biến thiết bị camera sử dụng |
| **Tài liệu hướng dẫn cài đặt bảo mật** | Tài liệu hướng dẫn cho người dùng cách thức cài đặt bảo mật cho thiết bị camera. |
| **Tài liệu hướng dẫn kiểm tra cài đặt** | Mô tả tài liệu hướng dẫn cho người dùng cách thức kiểm tra, rà soát cài đặt bảo mật của thiết bị camera. |
| **Tài liệu về dữ liệu cá nhân** | Tài liệu mô tả các thức camera thu thập và xử lý thông tin cá nhân.  |
| **Tài liệu về dữ liệu đo đạc từ xa** | Mô tả mô tả đầy đủ về mục đích, đối tượng thu thập và nơi lưu trữ các loại dữ liệu đo đạc từ xa trên thiết bị camera được thu thập bởi nhà sản xuất (nếu có). |
| **Tài liệu hướng dẫn về xóa dữ liệu cá nhân** | Tài liệu hướng dẫn cho người dùng cách thức xóa dữ liệu cá nhân được thu thập, xử lý bởi camera. |
| **Định danh thiết bị** | Tài liệu mô tả cách thức nhận biết thiết bị camera thông qua mã định danh thiết bị.  |
| **Thời gian hỗ trợ** | Thời gian thiết bị camera được nhà sản xuất duy trì hỗ trợ dịch vụ, ví dụ như cung cấp các bản cập nhật. |
| **Công bố thời gian hỗ trợ** | Mô tả cách thức công bố và thông tin cho người dùng về thời gian hỗ trợ sản phẩm. |
| **Chính sách công bố lỗ hổng** | Mô tả cách thức công bố và thông tin cho người dùng về lỗ hổng bảo mật liên quan đến thiết bị camera mà hãng sản xuất. |
| **Công bố không hỗ trợ** | Mô tả về các thành phần trên thiết bị camera không được nhà sản xuất hỗ trợ cập nhật. |

**IXIT 3-VulnTypes: Phân loại lỗ hổng bảo mật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phân loại lỗ hổng bảo mật trong bảng IXIT 3-VulnTypes. Ví dụ: VulnTypes-1, VulnTypes-2,... |
| **Mô tả** | Mô tả ngắn gọn về lỗ hổng bảo mật trong thiết bị camera. |
| **Hành động** | Mô tả quy trình xử lý bao gồm các bước thực hiện đối với phân loại lỗ hổng bảo mật này, bao gồm tất cả các thực thể và trách nhiệm thực hiện. |
| **Khung thời gian** | Khung thời gian dự kiến với các bước thực hiện trong quá trình xử lý lỗ hổng bảo mật. |

**IXIT 4-Conf: Cam kết bảo mật**

|  |  |
| --- | --- |
| **Xác nhận xử lý lỗ hổng (Có/Không)** | Xác nhận rằng đối với mỗi quy trình được mô tả trong IXIT 3-VulnTypes, cơ sở hạ tầng và nhân sự cần thiết được đảm bảo để đạt được khung thời gian dự kiến. |
| **Xác nhận giám sát lỗ hổng (Có/Không)** | Xác nhận rằng đối với việc giám sát, xác định và khắc phục lỗ hổng được mô tả trong IXIT 5-VulnMon, cơ sở hạ tầng và nhân sự cần thiết được đảm bảo. |
| **Xác nhận quy trình cập nhật (Có/Không)** | Xác nhận rằng đối với mỗi quy trình cập nhật được mô tả trong IXIT 8-UpdProc, cơ sở hạ tầng và nhân sự cần thiết được đảm bảo để đạt được khung thời gian dự kiến. |
| **Xác nhận quản lý bảo mật (Có/Không)** | Xác nhận rằng các quy trình quản lý bảo mật được mô tả trong IXIT 14-SecMgmt đã được triển khai. |
| **Xác nhận phát triển an toàn (Có/Không)** | Xác nhận rằng các quy trình phát triển an toàn được mô tả trong IXIT 19-SecDev đã được triển khai. |

**IXIT 5-VulnMon: Theo dõi xử lý lỗ hổng bảo mật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phương thức giám sát trong bảng IXIT 5-VulnMon. Ví dụ: VulnMon-1, VulnMon-2,... |
| **Mô tả** | Mô tả cách thức theo dõi việc xử lý và khắc phục lỗ hổng bảo mật đối với thiết bị camera. |

**IXIT 6-SoftComp: Các thành phần phần mềm**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi thành phần phần mềm trên thiết bị trong bảng IXIT 6-SoftComp. Ví dụ: SoftComp-1, SoftComp-2,... |
| **Mô tả** | Mô tả ngắn gọn về thành phần phần mềm trên thiết bị. Ví dụ: Firmware, Bootloader,... |
| **Cơ chế cập nhật** | Tham chiếu đến các cơ chế cập nhật trong IXIT 7-UpdMech được sử dụng để cập nhật cho thành phần phần mềm trên thiết bị. Nếu không có cơ chế cập nhật cho thành phần này, cần cung cấp lý do. |
| **Phương thức mã hóa** | Mô tả thành phần phần mềm trên thiết bị có sử dụng các thuật toán mã hóa hay không. Nếu sử dụng, mô tả các ảnh hưởng nếu có đối với thuật toán mã hóa sử dụng khi cập nhật phần mềm. |

**IXIT 7-UpdMech: Cơ chế cập nhật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế cập nhật trên thiết bị trong bảng IXIT 7-UpdMech. Ví dụ: UpdMech-1, UpdMech-2,... |
| **Mô tả** | Mô tả ngắn gọn về cơ chế, bác bước thiết bị thực hiện cập nhật. Chỉ rõ cơ chế cập nhật hỗ trợ, ví dụ trực tuyến, tự động hay thủ công. |
| **Điều kiện đảm bảo bảo mật** | Mô tả các điều kiện về bảo mật cần bảo đảm để cơ chế cập nhật được được thực hiện như được mô tả. |
| **Phương thức mã hóa** | Mô tả các phương pháp mã hóa (giao thức, hoạt động, nguyên tắc, chế độ và kích thước khóa) được sử dụng để đáp ứng các điều kiện bảo mật ở trên. |
| **Khởi tạo và tương tác** | Mô tả tương tác của người dùng cần thiết để khởi tạo và áp dụng bản cập nhật. |
| **Cấu hình** | Mô tả ngắn gọn về cách thức cấu hình cơ chế tự động cập nhật và thông báo cập nhật phần mềm cho người dùng. Cần mô tả thêm thông tin về cấu hình cập nhật mặc định. |
| **Kiểm tra cập nhật** | Mô tả ngắn gọn về thời gian định kỳ thiết bị kiểm tra các bản cập nhật mới. |
| **Thông báo người dùng** | Mô tả ngắn gọn cách thức người dùng được thông báo về bản cập nhật có sẵn và những gián đoạn gây ra bởi cơ chế cập nhật, ví dụ như các hạn chế trong tính năng cụ thể. Cần mô tả thêm về giao diện và nội dung thông báo. |

**IXIT 8-UpdProc: Quy trình cập nhật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi quy trình công bố bản cập nhật trong bảng IXIT 8-UpdProc. Ví dụ: UpdProc-1, UpdProc-2,... |
| **Mô tả** | Mô tả ngắn gọn về quy trình triển khai và công bố bản cập nhật bao gồm tất cả các thực thể và trách nhiệm thực hiện. |
| **Khung thời gian** | Khung thời gian dự kiến để hoàn thành quy trình. |

**IXIT 9-ReplSup: Bảo trì thiết bị**

|  |  |
| --- | --- |
| **Cách ly** | Mô tả quy trình bao gồm các bước thực hiện để cách ly thiết bị camera. |
| **Thay thế phần cứng** | Mô tả quy trình bao gồm các bước thực hiện để thay thế phần cứng thiết bị camera. |

**IXIT 10-SecParam: Tham số bảo mật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi tham số bảo mật trong bảng IXIT 10-SecParam. Ví dụ: SecParam-1, SecParam-2,... |
| **Mô tả** | Mô tả ngắn gọn về tham số bảo mật và mục đích sử dụng. Cần mô tả thêm nếu tham số được mã hóa cứng và/hoặc mã hóa cứng trong mã nguồn phần mềm trên thiết bị. |
| **Loại** | Xác nhận tham số bảo mật là công khai hay quan trọng. |
| **Điều kiện đảm bảo bảo mật** | Mô tả cách thức bảo vệ tham số bảo mật trước các mối đe dọa trong quá trình lưu trữ lâu dài. |
| **Biện pháp bảo vệ** | Mô tả các biện pháp được áp dụng để bảo vệ tham số bảo mật. Điều này bao gồm các nguyên tắc, vai trò và quyền hạn đối với các vai trò được phép truy cập vào tham số. |
| **Cơ chế cung cấp** | Nếu tham số bảo mật thuộc loại quan trọng: Mô tả tác động của tham số đó đối với thiết bị camera. |
| **Cơ chế kết nối** | Tham chiếu đến các cơ chế kết nối trong IXIT 11-ComMech được sử dụng để truyền nhận tham số và xác nhận (Có/Không) rằng việc giao tiếp được thực hiện qua các giao diện truy cập từ xa (như Internet) |
| **Cơ chế khởi tạo** | Nếu tham số bảo mật thuộc loại quan trọng và 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: Mô tả cơ chế khởi tạo các giá trị của tham số và mô tả mục đích sử dụng. |

**IXIT 11-ComMech: Cơ chế kết nối**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế kết nối trong bảng IXIT 11-ComMech. Ví dụ: ComMech-1, ComMech-2,.... |
| **Mô tả** | Mô tả ngắn gọn về cơ chế kết nối, bao gồm mục đích và mô tả giao thức được sử dụng. Cần mô tả thêm nếu cơ chế có thể truy cập từ xa. |
| **Điều kiện đảm bảo bảo mật** | Mô tả cách thức bảo vệ cơ chế kết nối trước các mối đe dọa. |
| **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 kết nối bao gồm cách thức quản lý khóa và hỗ trợ các nguyên tắc đảm bảo bảo mật được mô tả bên trên. |
| **Biện pháp khôi phục** | Mô tả cách thức đảm bảo kết nối ổn định bao gồm trạng thái dự kiến, hoạt động và biện pháp khôi phục. |

**IXIT 12-NetSecImpl: Bảo mật đường truyền mạng**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phương thức bảo mật đường truyền mạng trong bảng IXIT 12-NetSecImpl. Ví dụ: NetSecImpl-1, NetSecImpl-2,... |
| **Mô tả** | Mô tả ngắn gọn về chức năng hoặc phương thức bảo mật trên đường truyền mạng, bao gồm mục đích sử dụng và phạm vi của nó. |
| **Phương pháp thực hiện** | Mô tả phương pháp thực hiện (ví dụ: kiểm toán, rà soát đường truyền, phân tích mã tự động, sử dụng công cụ). Cần mô tả thêm về phạm vi triển khai và phạm vi áp dụng. |
| **Báo cáo** | Mô tả kết quả của việc triển khai theo phương pháp bên trên hoặc tham chiếu đến chứng chỉ hoặc báo cáo chứng minh phương pháp được thực hiện thành công. |

**IXIT 13-SoftServ: Dịch vụ phần mềm**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi dịch vụ được cung cấp bởi phần mềm trên thiết bị trong bảng IXIT 13-SoftServ. Ví dụ: SoftServ-1, SoftServ-2,... |
| **Mô tả** | Mô tả ngắn gọn về dịch vụ và mục đích sử dụng. Cần mô tả thêm nếu dịch vụ có thể truy cập qua kết nối mạng và có thể sử dụng trong trạng thái đã khởi tạo không. |
| **Trạng thái (Bật/Tắt)** | Xác nhận dịch vụ được bật hay tắt trong trạng thái đã khởi tạo. |
| **Giải thích** | Nếu dịch vụ được bật: Giải thích lý do tại sao dịch vụ là cần thiết cho mục đích sử dụng hoặc vận hành của thiết bị camera. |
| **Cho phép cấu hình (Có/Không)** | Nếu dịch vụ có thể truy cập qua giao diện mạng: Xác nhận (Có/Không) rằng dịch vụ có khả năng thay đổi cấu hình liên quan đến bảo mật. Nếu có, mô tả ngắn gọn về các cấu hình có thể thực hiện. |
| **Cơ chế xác thực** | Nếu dịch vụ có thể truy cập qua giao diện mạng: Tham chiếu đến các cơ chế xác thực trong IXIT 1-AuthMech được sử dụng để xác thực trước khi sử dụng dịch vụ. |

**IXIT 14-SecMgmt: Quy trình quản lý bảo mật**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi quy trình quản lý bảo mật trong bảng IXIT 14-SecMgmt. Ví dụ: SecMgmt-1, SecMgmt-2,... |
| **Mô tả** | Mô tả ngắn gọn về quy trình quản lý bảo mật để bảo vệ các tham số bảo mật quan trọng. Nếu một tiêu chuẩn hiện có được sử dụng, cung cấp tham chiếu đến tiêu chuẩn tương ứng. |

**IXIT 15-Intf: Giao diện**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi giao diện trong bảng IXIT 15-Intf. Ví dụ: Intf-1, Intf-2,... |
| **Mô tả** | Mô tả ngắn gọn về giao diện bao gồm mục đích sử dụng. Đối với các giao diện vật lý, mô tả thêm liệu giao diện đó cần thiết, không cần thiết hay chỉ cần thiết trong các trường hợp cụ thể (ví dụ: sử dụng trong quá trình phát triển). |
| **Loại** | Xác nhận giao diện là giao diện mạng, giao diện vật lý (bao gồm cả giao diện không dây), giao diện logic hay nhiều loại. |
| **Tình trạng (Kích hoạt/Không kích hoạt)** | Xác nhận giao diện được kích hoạt hay không trong trạng thái khởi tạo. Đối với các giao diện được kích hoạt, cung cấp lý do. |
| **Thông tin có thể tiết lộ** | Nếu giao diện là giao diện mạng: Mô tả thông tin được tiết lộ mà không cần xác thực trong trạng thái khởi tạo và lý do cho việc tiết lộ. Xác nhận rằng thông tin có ảnh hưởng đến bảo mật hay không. |
| **Giao diện gỡ lỗi** | Nếu giao diện là giao diện vật lý: Xác nhận rằng giao diện có thể được sử dụng như một 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 sự tiếp xúc với giao diện. |

**IXIT 16-CodeMin: Tối ưu mã nguồn**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phương pháp tối ưu mã nguồn trong bảng IXIT 16-CodeMin. Ví dụ: CodeMin-1, CodeMin-2,... |
| **Mô tả** | Mô tả ngắn gọn về phương thức và công cụ tối ưu hóa mã nguồn. |

**IXIT 17-PrivlCtrl: Kiểm soát phân quyền**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế kiểm soát quyền hạn trong bảng IXIT 17-PrivlCtrl. Ví dụ: PrivlCtrl-1, PrivlCtrl-2,... |
| **Mô tả** | Mô tả ngắn gọn về cơ chế kiểm soát quyền hạn của phần mềm trên thiết bị camera. |

**IXIT 18-AccCtrl: Kiểm soát truy cập**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế kiểm soát truy cập trong bảng IXIT 18-AccCtrl. Ví dụ: AccCtrl-1, AccCtrl-2,... |
| **Mô tả** | Mô tả ngắn gọn về cơ chế kiểm soát truy cập của phần cứng trên thiết bị camera. Mô tả cách thức hệ điều hành của thiết bị camera hỗ trợ cơ chế này. |

**IXIT 19-SecDev: Quy trình phát triển phần mềm an toàn**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi quy trình phát triển phần mềm trên thiết bị camera trong bảng IXIT 19-SecDev. Ví dụ: SecDev-1, SecDev-2,... |
| **Mô tả** | Mô tả ngắn gọn về quy trình phát triển phần mềm trên thiết bị camera an toàn. Nếu một tiêu chuẩn hiện có được sử dụng, cung cấp tham chiếu đến tiêu chuẩn tương ứng. |

**IXIT 20-SecBoot: Cơ chế khởi động thiết bị an toàn**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế khởi động bảo mật trong bảng IXIT 20-SecBoot. Ví dụ: SecBoot-1, SecBoot-2,... |
| **Mô tả** | Mô tả ngắn gọn về quy trình khởi động bảo mật của thiết bị camera bao gồm các cơ chế liên quan và mô tả những thành phần nào được bảo vệ. |
| **Điều kiện bảo đảm bảo mật** | Mô tả cách thức bảo vệ cơ chế khởi động thiết bị trước các mối đe dọa. |
| **Cơ chế phát hiện vi phạm** | Mô tả cơ chế phát hiện thay đổi trái phép trong phần mềm của thiết bị camera. |
| **Thông báo cho người dùng** | Mô tả ngắn gọn cách người dùng được thông báo về sự thay đổi trái phép trong phần mềm. Đồng thời, mô tả nội dung trong thông báo. |
| **Chức năng thông báo** | Mô tả ngắn gọn các chức năng mạng cần thiết để thông báo cho người dùng. |

**IXIT 21-PersData: Dữ liệu cá nhân**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi phân loại dữ liệu cá nhân người sử dụng trong bảng IXIT 21-PersData. Ví dụ: PersData-1, PersData-2,.... |
| **Mô tả** | Mô tả ngắn gọn về phân loại dữ liệu cá nhân được thiết bị camera xử lý. |
| **Hành động** | Mô tả cách thức xử lý dữ liệu cá nhân bao gồm tất cả các bên liên quan. Đồng thời, mô tả các mục đích của việc xử lý. |
| **Cơ chế kết nối** | Tham chiếu đến các cơ chế kết nối trong IXIT 11-ComMech được sử dụng để truyền dữ liệu cá nhân và xác nhận (Có/Không) rằng đối tác giao tiếp là dịch vụ liên kết. |
| **Tính nhạy cảm (Có/Không)** | Xác nhận rằng dữ liệu cá nhân thuộc loại nhạy cảm hay không. |
| **Thu thập sự đồng ý** | Nếu dữ liệu cá nhân được xử lý dựa trên sự đồng ý của người sử dụng: Mô tả cách thức thu thập sự đồng ý từ người sử dụng. |
| **Rút lại sự đồng ý** | Nếu dữ liệu cá nhân được xử lý dựa trên sự đồng ý của người sử dụng: Mô tả cách người sử dụng có thể rút lại sự đồng ý. |

**IXIT 22-ExtSens: Cảm biến bên ngoài**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cảm biến bên ngoài trên thiết bị camera trong bảng IXIT 22-ExtSens. Ví dụ: ExtSens-1, ExtSens-2,... |
| **Mô tả** | Mô tả ngắn gọn về các cảm biến. |

**IXIT 23-ResMech: Cơ chế khôi phục sau sự cố**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế khôi phục sau sự cố trong bảng IXIT 23-ResMech. Ví dụ: ResMech-1, ResMech-2,... |
| **Mô tả** | Mô tả cơ chế khôi phục của thiết bị camera đối với sự cố mất kết nối mạng và/hoặc mất điện. |
| **Loại** | Xác nhận vấn đề được cơ chế khôi phục giải quyết. Ví dụ: vấn đề kết nối mạng, mất điện hay cả hai. |
| **Điều kiện bảo đảm bảo mật** | Mô tả cách thức cơ chế khôi phục bảo vệ thiết bị trước các mối đe dọa. |

**IXIT 24-TelData: Dữ liệu đo đạc từ xa**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi cơ chế khôi phục sau sự cố trong bảng IXIT 24-TelData. Ví dụ: TelData-1, TelData-2,... |
| **Mô tả** | Mô tả ngắn gọn về dữ liệu chẩn đoán được thu thập bởi thiết bị camera và cung cấp cho nhà sản xuất. |
| **Mục đích** | Mô tả ngắn gọn mục đích thu thập dữ liệu. |
| **Kiểm tra an ninh** | Nếu dữ liệu được sử dụng cho mục đích kiểm tra sau khi phát hiện sự cố an ninh: Mô tả cách thức kiểm tra dữ liệu chẩn đoán để phát hiện bất thường về mất an toàn thông tin, bao gồm các bên liên quan. |
| **Dữ liệu cá nhân** | Tham chiếu đến dữ liệu cá nhân trong IXIT 21-PersData được xử lý trong dữ liệu chẩn đoán. |

**IXIT 25-DelFunc: Chức năng hủy bỏ và khôi phục cài đặt gốc**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi chức năng hủy bỏ và khôi phục cài đặt gốc trong bảng IXIT 25-DelFunc. Ví dụ: DelFunc-1, DelFunc-2,... |
| **Mô tả** | Mô tả ngắn gọn về chức năng xóa dữ liệu trên thiết bị. Mô tả tác động tới dịch vụ liên kết nếu có liên quan. |
| **Đối tượng** | Xác nhận chức năng xử lý dữ liệu người dùng trên thiết bị, dữ liệu cá nhân trên dịch vụ liên kết, hay cả hai. |
| **Khởi tạo và tương tác** | Mô tả ngắn gọn về tương tác của người dùng cần thiết để khởi tạo và áp dụng chức năng hủy bỏ và khôi phục cài đặt gốc. |
| **Xác nhận** | Mô tả ngắn gọn cách thức mà người dùng được thông báo rằng dữ liệu được đề cập đã được xóa sau khi áp dụng chức năng hủy bỏ và khôi phục cài đặt gốc. |

**IXIT 26-UserDec: Tương tác của người dùng**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi tương tác của người dùng trong bảng IXIT 26-UserDec. Ví dụ: UserDec-1, UserDec-2,... |
| **Mô tả** | Mô tả về các quyết định cần được người dùng thực hiện trong quá trình cài đặt và bảo trì thiết bị camera. |
| **Tùy chọn** | Mô tả các tùy chọn bảo mật mà người dùng có thể lựa chọn và chỉ định giá trị mặc định. |
| **Kích hoạt (Có/Không)** | Mô tả ngắn gọn cách quyết định được kích hoạt khi có tương tác của người dùng. Xác nhận quyết định có thể được người dùng kích hoạt hay không. |

**IXIT 27-UserIntf: Giao diện người dùng**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi giao diện người sử dụng trong bảng IXIT 27-UserIntf. Ví dụ: UserIntf-1, UserIntf-2,... |
| **Mô tả** | Mô tả ngắn gọn về giao diện cho phép nhập dữ liệu từ người sử dụng. Xác nhận việc truy cập giao diện có thể được thực hiện bởi người sử dụng. |

**IXIT 28-ExtAPI: Dịch vụ liên kết**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi dịch vụ liên kết trong bảng IXIT 28-ExtAPI. Ví dụ: ExtAPI-1, ExtAPI-2,... |
| **Mô tả** | Mô tả về các giao thức API cho phép truy nhập dữ liệu từ các dịch vụ liên kết của thiết bị camera. |

**IXIT 29-InpVal: Kiểm tra dữ liệu đầu vào**

|  |  |
| --- | --- |
| **ID** | Mã định danh mỗi dịch vụ liên kết trong bảng IXIT 29-InpVal. Ví dụ: InpVal-1, InpVal-2,... |
| **Mô tả** | Mô tả về phương thức kiểm tra dữ liệu đầu vào qua các giao diện người dùng, hoặc qua các giao thức API và giữa các kết nối mạng trong các dịch vụ và thiết bị. Cần mô tả thêm các nguồn đầu vào dữ liệu được xử lý. |

PHỤ LỤC B

**(Tham khảo)**

**DANH MỤC VÍ DỤ THÔNG TIN PHỤC VỤ ĐÁNH GIÁ**

**Bảng C.1: Mẫu IXIT 1-AuthMech (Cơ chế xác thực)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Giá trị xác thực** | **Cơ chế khởi tạo mật khẩu** | **Điều kiện đảm bảo bảo mật** | **Phương thức mã hóa** | **Ngăn chặn tấn công vét cạn** |
| AuthMech-1 | Người dùng có thể đăng nhập qua HTTPS tại cổng 443 để truy cập vào giao diện web. (Người dùng có thể yêu cầu đăng nhập qua HTTP tại cổng 80 nhưng sẽ tự động chuyển tiếp sang HTTPS trên cổng 443.) Việc xác thực trên trang đăng nhập phải được hoàn tất trước khi bất kỳ tải xuống dữ liệu nào qua HTTPS được trao đổi. Không có dữ liệu tải xuống nào có thể đọc được nếu trước đó chưa đăng nhập. Máy chủ web xác thực thông tin đăng nhập đã được cung cấp để thông tin đăng nhập được lưu trữ trong cơ sở dữ liệu SQLite của nó và cấp quyền truy cập vào các tài nguyên được yêu cầu. Cơ chế này được sử dụng cho người dùng xác thực với máy chủ. Cơ chế này có thể truy cập trực tiếp từ một mạng giao diện. | Tên người dùng và mật khẩu (được cài đặt sẵn và sử dụng trong trạng thái khởi động). | Tên người dùng được cố định là "admin". Mật khẩu được tạo ngẫu nhiên và duy nhất cho mỗi thiết bị. Mật khẩu có độ dài 16 ký tự, bao gồm các ký tự chữ hoa, chữ thường và số. Mật khẩu được tạo bằng cách sử dụng `/dev/urandom` trên UNIX cấu hình hệ thống trong giai đoạn sản xuất. | Tên người dùng và mật khẩu được truyền qua kênh HTTPS, do đó, Thiết bị Thiết bị camera đảm bảo bảo mật và an toàn trong quá trình truyền tải. | Xác thực xác thực dựa trên biểu mẫu HTML bằng cách sử dụng một tập lệnh PHP kết hợp với cơ sở dữ liệu SQLite. Tính toàn vẹn và bảo mật của quá trình truyền mật khẩu đến thiết bị camera được đảm bảo qua TLS 1.2. Theo mặc định, thiết bị camera cung cấp bộ mã hóa sau cho quá trình bắt tay TLS: ECDHE-ECDSA-AES128-GCM-SHA256 hoặc ECDHE-ECDSA-AES256-GCM-SHA384. | Sau 3 lần đăng nhập không hợp lệ, thông tin đăng nhập của giao diện sẽ không thể truy cập được trong 5 phút. |

**Bảng C.2: Mẫu IXIT 2-UserInfo (Thông tin cung cấp cho người dùng)**

|  |  |
| --- | --- |
| **Tài liệu hướng dẫn thay đổi thông tin xác thực** | Người dùng có thể tìm thấy thông tin để thay đổi các giá trị xác thực trong sổ tay hướng dẫn sử dụng Tệp PDF IPC 2000 có thể tải xuống trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip-Camera-example. Thông tin sản phẩm được in có chứa URL này trong phần 3. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Menu". |
| **Tài liệu hướng dẫn bảo trì thiết bị** | Không áp dụng (Không có thành phần nào không thể cập nhật) |
| **Tài liệu mô tả về các cảm biến camera sử dụng** | Chức năng micrô, chức năng máy ảnh (phổ nhìn thấy được) và chức năng máy ảnh (phổ hồng ngoại) được giải thích trên trang web sản phẩm của Nhà cung cấp, có thể truy cập tại https://example.net/support/devices/ip-máy ảnh-example . Thông tin sản phẩm được in có chứa URL này trong phần 9. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Tổng quan về chức năng". |
| **Tài liệu hướng dẫn cài đặt bảo mật** | Người dùng được hướng dẫn thông qua trình hướng dẫn thiết lập cho mỗi hộp thoại được xác định trước sau khi thay đổi mật khẩu ban đầu. Bằng các hộp thoại này, đảm bảo rằng người dùng không thể thực hiện cấu hình không an toàn trong quá trình thiết lập. Các hộp thoại được ghi lại trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip-Camera-example. Thông tin sản phẩm được in có chứa URL này trong phần 1. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Cài đặt". |
| **Tài liệu hướng dẫn kiểm tra cài đặt** | Mọi đầu vào của người dùng đều được kiểm tra theo các quy tắc xác thực. Tùy chọn duy nhất mà người dùng có thể đưa ra lựa chọn không an toàn là mật khẩu cho tài khoản người dùng mới. Nếu mật khẩu đã nhập không tuân thủ các quy tắc mật khẩu, người dùng sẽ được thông báo ngay lập tức qua giao diện web hoặc Ứng dụng và quy trình thiết lập không thể tiếp tục cho đến khi người dùng chọn đầu vào hợp lệ.Các hộp thoại được ghi lại trên trang web của Nhà cung cấp, có thể truy cập trong ví dụ https://example.net/support/devices/ip-Camera.Thông tin sản phẩm được in có chứa URL này trong phần 1. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Cài đặt". |
| **Tài liệu về dữ liệu cá nhân** | Người dùng có thể tìm thấy thông tin này trong sổ tay hướng dẫn sử dụng Tệp PDF IPC 2000 có thể tải xuống trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip-Camera-example. Thông tin sản phẩm được in có chứa URL này trong phần 6. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Đặt lại". |
| **Tài liệu về dữ liệu đo đạc từ xa** | Người dùng có thể tìm thấy thông tin này trong sổ tay hướng dẫn sử dụng Tệp PDF IPC 2000 có thể tải xuống trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip-Camera-example.Thông tin sản phẩm được in có chứa URL này trong phần 6. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Đặt lại". |
| **Tài liệu hướng dẫn về xóa dữ liệu cá nhân** | Người dùng có thể tìm thấy thông tin này trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip camera-example. Thông tin sản phẩm được in có chứa URL này trong phần 7. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Đặt lại" và "Trợ giúp" -> "Xóa tài khoản". |
| **Định danh thiết bị** | Ký hiệu model "IPC 2000" được cung cấp cho người dùng ở dưới cùng của hộp thiết bị camera ở dạng văn bản thuần túy. Ngoài ra, bạn có thể đọc chỉ định từ ứng dụng trong phần "Trợ giúp" -> "Giới thiệu" và từ giao diện web trong phần "Thiết bị". |
| **Thời gian hỗ trợ** | thiết bị camera này được duy trì tích cực liên quan đến các bản cập nhật bảo mật trong 6 năm tiếp theo sau khi đưa ra thị trường. |
| **Công bố thời gian hỗ trợ** | Người dùng có thể tìm thấy thông tin này trên trang web của Nhà cung cấp, có thể truy cập theo https://example.net/support/devices/ip camera-example. Thông tin sản phẩm được in có chứa URL này trong phần 4. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Chính sách bảo mật". |
| **Chính sách công bố lỗ hổng** | Người dùng có thể truy xuất chính sách tiết lộ lỗ hổng bảo mật từ trang web của Nhà cung cấp, có thể truy cập theo https://example.net/security/disclosure-policy. Thông tin sản phẩm được in có chứa URL này trong phần 3. Ngoài ra, URL này có thể được truy cập trực tiếp thông qua ứng dụng camera IP trong phần "Trợ giúp" -> "Chính sách bảo mật". Trên trang này, người dùng cũng tìm thấy biểu mẫu liên hệ để gửi các lỗi bảo mật tiềm ẩn cho thiết bị camera. |
| **Công bố không hỗ trợ** | Không áp dụng (Không có thành phần nào không thể cập nhật) |

**Bảng C.3: Mẫu IXIT 3-VulnTypes (Phân loại lỗ hổng bảo mật)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Mô tả** | **Hành động** | **Khung thời gian** |
| VulnTypes-1 | Các lỗ hổng trên giao diện người dùng web liên quan đến HTTP, PHP hoặc HTML và việc tích hợp vào các thành phần liên quan (máy chủ web, cơ sở dữ liệu, hệ điều hành và các thư viện đã sử dụng). | Khi nhận được thông báo về lỗ hổng bảo mật tiềm ẩn qua biểu mẫu liên hệ theo Chính sách tiết lộ lỗ hổng bảo mật, thông báo sẽ được chuyển tiếp đến Nhóm ứng cứu sự cố bảo mật để điều tra. Nếu cần, nhóm sẽ liên hệ với người dùng đã gửi biểu mẫu ban đầu để trao đổi thêm thông tin về lỗ hổng. Nếu nhóm xác nhận lỗ hổng, nó sẽ đề xuất bản sửa lỗi cho bộ phận Phát triển Phần mềm. Bộ phận sau đó sẽ thực hiện sửa lỗi và xác minh tính hiệu quả bên trong. Sau khi cả hai nhóm xác nhận rằng lỗ hổng đã được khắc phục, chương trình cơ sở mới sẽ được triển khai và nhật ký thay đổi cập nhật được xuất bản kèm theo mô tả về lỗ hổng đã được vá. | 7 ngày cho phản hồi ban đầu, 30 ngày để Nhóm ứng cứu sự cố bảo mật điều tra và đề xuất cách khắc phục, 30 ngày để bộ phận Phát triển Phần mềm tích hợp bản sửa lỗi. Chậm nhất là 90 ngày sau khi nhận được lỗ hổng, bản sửa lỗi sẽ được phát hành theo chính sách tiết lộ lỗ hổng đã công bố. |

**Bảng C.4: Mẫu IXIT 4-Conf (Cam kết bảo mật)**

|  |  |
| --- | --- |
| **Xác nhận xử lý lỗ hổng (Có/Không)** | Có |
| **Xác nhận giám sát lỗ hổng (Có/Không)** | Có |
| **Xác nhận quy trình cập nhật (Có/Không)** | Có |
| **Xác nhận quản lý bảo mật (Có/Không)** | Có |
| **Xác nhận phát triển an toàn (Có/Không)** | Có |

**Bảng C.5: Mẫu IXIT 5-VulnMon (Theo dõi xử lý lỗ hổng bảo mật)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| VulnMon-1 | Nhà cung cấp giám sát các trang web CVE https://www.cvedetails.com/ và https://cve.mitre.org/ để tìm các lỗ hổng ảnh hưởng đến các thành phần được sử dụng cho thiết bị camera. Hơn nữa, các nhà cung cấp các thành phần phần mềm đã qua sử dụng cho thiết bị camera đã cam kết công bố các lỗ hổng bảo mật trên các trang CVE này. Nhóm Sự cố Bảo mật kiểm tra cả hai địa điểm hàng tuần. Khi phát hiện được lỗ hổng tiềm ẩn, SIT sẽ tiếp tục quy trình được mô tả trong IXIT 3 VulnTypes. Nếu một lỗ hổng được liệt kê trên một hoặc cả hai trang web được đề cập nhưng không áp dụng được cho thiết bị camera thì CVE sẽ được ghi chú nội bộ là "n/a" để ghi lại rằng lỗ hổng đó đã được điều tra. |
| VulnMon-2 | Nhà cung cấp giám sát các trang web sau để tìm thông tin xác thực bị rò rỉ hoặc thông tin nhạy cảm khác có thể được truy nguyên một cách rõ ràng về thiết bị camera: https://one.example.net, https://two.example.net. Nếu có phát hiện, nhân viên quyền riêng tư của Nhà cung cấp có trách nhiệm điều tra thêm vấn đề này để xác nhận hoặc từ chối rằng các biện pháp tiếp theo liên quan đến quyền riêng tư là cần thiết. Trong trường hợp trước, thủ tục phụ thuộc vào vấn đề cụ thể và các quy định của chính phủ. Nếu sự cố ảnh hưởng đến những người dùng có thể nhận dạng của thiết bị camera, Nhóm Sự cố Bảo mật sẽ tham gia thông báo cho khách hàng đã đăng ký về sự cố. |

**Bảng C.6: Mẫu IXIT 6-SoftComp (Các thành phần phần mềm)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Mô tả** | **Cơ chế cập nhật** | **Phương thức mã hóa** |
| SoftComp-1 | Phần mềm bao gồm hệ điều hành dựa trên Linux, thư viện mật mã OpenSSL, Máy chủ web Apache bao gồm PHP và SQLite, nhiều thư viện khác nhau. | Firmware có thể được cập nhật theo UpdMech-1, UpdMech-2 và UpdMech-3. | Có, phần mềm bao gồm các thuật toán mã hóa có sẵn cho thiết bị camera. Có, tác dụng của việc cập nhật các thuật toán và các thành phần được nhà sản xuất xem xét thông qua việc kiểm tra toàn diện các giao diện của thiết bị camera bởi Phòng Phát triển Phần mềm. |

**Bảng C.7: Mẫu IXIT 7-UpdMech (Cơ chế cập nhật)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Điều kiện đảm bảo bảo mật** | **Phương thức mã hóa** | **Khởi tạo và tương tác** | **Cấu hình** | **Kiểm tra cập nhật** | **Thông báo người dùng** |
| UpdMech-1 | Cập nhật chương trình cơ sở do người dùng thực hiện qua giao diện web. thiết bị camera truy vấn máy chủ cập nhật https://update.example.net để xác minh xem có bản cập nhật hay không. Việc này được thực hiện tự động một lần mỗi ngày. Nếu có bản cập nhật, thiết bị camera sẽ thông báo cho người dùng về nó hoặc tự động bắt đầu cập nhật, tùy thuộc vào cấu hình của nó. Khi người dùng hoặc chính thiết bị camera khởi động cơ chế cập nhật, máy chủ sẽ cung cấp bản cập nhật cho thiết bị camera qua kết nối mạng của nó. Gói cập nhật được mã hóa bằng khóa đối xứng tĩnh. thiết bị camera giải mã gói cập nhật, sau đó xác minh tính xác thực và tính toàn vẹn của bản cập nhật được giải mã bằng khóa bất đối xứng và quá trình cài đặt được bắt đầu. Sau khi cập nhật xong, người dùng sẽ được thông báo cập nhật thành công. | Cơ chế cập nhật cung cấp tính bảo mật bằng cách mã hóa gói cập nhật. Khóa mã hóa được sử dụng là khóa AES được mã hóa cứng (bản thân khóa này cũng có thể cập nhật được) của máy chủ cập nhật. thiết bị camera xác minh tính toàn vẹn và tính xác thực của tệp cập nhật dựa trên khóa chung RSA được mã hóa cứng (bản thân nó cũng có thể cập nhật được) của máy chủ cập nhật. | Tính bảo mật của bản cập nhật phần mềm được thực hiện bằng gói chương trình cơ sở được mã hóa dựa trên 10.6028/NIST.FIPS.197. Để giải mã, AES-CBC với 128 bit được sử dụng, phù hợp với Cơ chế đánh giá mật mã SOG-IS đã được thống nhất, Phiên bản 1.2. Tính xác thực và tính toàn vẹn của bản cập nhật phần mềm được thực hiện bằng gói chương trình cơ sở đã ký dựa trên IETF RFC 8017. Đối với chữ ký SHA-512 có RSA 4096 bit và OAEP được sử dụng. Việc ký gói chương trình cơ sở được thực hiện bằng khóa riêng của máy chủ cập nhật. Khóa chung để xác thực bản cập nhật được tích hợp trong quá trình sản xuất thiết bị camera và được mã hóa cứng trong phần mềm. thiết bị camera ngăn chặn cuộc tấn công hạ cấp bằng cách xác minh rằng phiên bản của gói chương trình cơ sở mới không thể thấp hơn phiên bản của gói chương trình cơ sở hiện được cài đặt. | thiết bị camera tự động kiểm tra mỗi ngày một lần (thời gian được chọn ngẫu nhiên cho mỗi ngày) để tìm các bản cập nhật chương trình cơ sở được lưu trữ tại https://update.example .net. Người dùng sẽ được thông báo khi có bản cập nhật. Sau đó, người dùng có thể kích hoạt cập nhật bằng cách đăng nhập vào giao diện web và bắt đầu quá trình cập nhật theo cách thủ công bằng cách nhấn nút "Áp dụng cập nhật và khởi động lại" hoặc thiết bị camera tự động bắt đầu cập nhật, tùy thuộc vào cấu hình của nó. Sau khi bắt đầu cập nhật, nó sẽ tiếp tục mà không có bất kỳ sự tương tác nào của người dùng. | Người dùng có thể định cấu hình thiết bị camera để bắt đầu cập nhật tự động khi có sẵn. Tùy chọn mặc định là người dùng chỉ được thông báo về bản cập nhật và kích hoạt nó theo cách thủ công. Trong trường hợp này, người dùng sẽ được hỏi liệu bản cập nhật nên được cài đặt ngay bây giờ hay vào một ngày sau đó ("cài đặt ngay" hoặc "hoãn"). | thiết bị camera liên hệ với máy chủ cập nhật tại https://upda te.example. net một lần mỗi ngày (thời gian được chọn ngẫu nhiên cho mỗi ngày). Nếu không thể truy cập máy chủ, quá trình kiểm tra cập nhật sẽ bị hoãn lại trong 2 giờ. thiết bị camera khởi tạo và thực hiện kiểm tra cập nhật. | Người dùng được thông báo qua ứng dụng (bằng tin nhắn đẩy) về bản cập nhật đang chờ xử lý. Người dùng cũng được thông báo sau khi đăng nhập trên giao diện web. Thông báo bao gồm: • thời gian ước tính cần thiết để áp dụng bản cập nhật • cảnh báo rằng trong thời gian này các dịch vụ sẽ không khả dụng • nhật ký thay đổi ngắn gọn về những thay đổi quan trọng nhất. Các thông báo trên giao diện web được chính thiết bị camera thực hiện. |

**Bảng C.8: Mẫu IXIT 8-UpdProc (Quy trình cập nhật)**

|  |  |  |
| --- | --- | --- |
| **ID** | **Mô tả** | **Khung thời gian** |
| UpdProc-1 | Mọi bản phát hành chương trình cơ sở của thiết bị camera đều thuộc trách nhiệm của Nhóm Phát triển Phần mềm. Nhóm chịu trách nhiệm tích hợp các bản sửa lỗi bảo mật và kiểm tra chương trình cơ sở bằng các bài kiểm tra tích cực và tiêu cực. Sau khi thay đổi được xác minh và kiểm tra, nhóm sẽ tung ra bản cập nhật trên máy chủ cập nhật chính thức. Để phối hợp xử lý các bản sửa lỗi bảo mật, nhóm sử dụng hệ thống yêu cầu nội bộ để không bản sửa lỗi bảo mật nào bị bỏ qua. Những thay đổi liên quan đến mỗi bản phát hành chương trình cơ sở được nhóm ghi lại trong nhật ký thay đổi, được công bố trên trang web của sản phẩm. | Như đã đề cập trong VulnTypes-1, thời gian đưa ra phần mềm cơ sở mới là 30 ngày. |

**Bảng C.9: Mẫu IXIT 9-ReplSup (Bảo trì thiết bị)**

|  |  |
| --- | --- |
| **Cách ly** | Cảm biến cửa sổ có thể bị ngắt kết nối khỏi mạng trong Smart Hub mà nó được kết nối. Sau đó, tín hiệu từ cảm biến cửa sổ không thể ảnh hưởng đến mạng nữa. Trong trường hợp này, cảm biến cửa sổ vẫn giữ chức năng cốt lõi là thông báo cho người dùng về việc mở hoặc đóng cửa sổ bằng một âm thanh ngắn phát ra trong trường hợp xảy ra sự kiện như vậy. |
| **Thay thế phần cứng** | Cảm biến cửa sổ có thể được thay thế toàn bộ bằng một thiết bị cảm biến cửa sổ mới, sau đó được kết nối với mạng mới thay vì mạng cũ. |

**Bảng C.10: Mẫu IXIT 10-SecParam (Tham số bảo mật)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Loại** | **Điều kiện đảm bảo bảo mật** | **Biện pháp bảo vệ** | **Cơ chế cung cấp** | **Cơ chế kết nối** | **Cơ chế khởi tạo** |
| SecParam-1 | Khóa chữ ký công khai RSA của máy chủ cập nhật để xác minh tính xác thực và tính toàn vẹn của các bản cập nhật chương trình cơ sở (sau giải mã với SecParam-2). Chìa khóa không phải là danh tính được mã hóa cứng. Chìa khóa được mã hóa cứng trong mã nguồn phần mềm thiết bị. | Công cộng | Chìa khóa không phải là có thể sửa đổi bởi một kẻ tấn công vậy mà tính toàn vẹn của nó được đảm bảo. | Người dùng đáng tin cậy không có quyền truy cập đến khóa thông qua bất kỳ giao diện nào.Người dùng không đáng tin cậy cần quyền truy cập root để dừng quá trình cập nhật và thay đổi chìa khóa.Vai trò người dùng duy nhất có quyền truy cập để đọc và sửa đổi khóa là quá trình cập nhật phần mềm. | Không áp dụng(Không cung cấp) | Không áp dụng(Không truyền đi) | Không áp dụng(Không cung cấp) |

**Bảng C.11: Mẫu IXIT 11-ComMech (Cơ chế kết nối)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Đảm bảo an ninh** | **Phương thức mã hóa** | **Biện pháp khôi phục** |
| ComMech-1 | Thiết bị camera cung cấp một kết nối cho giao diện web trong môi trường mạng LAN như máy chủ. Kết nối này dựa trên IP/TCP/HTTPS. Cơ chế là có thể truy cập từ xa. | Thông qua TLS đảm bảo truyền thông tính xác thực của thiết bị camera, tính toàn vẹn và bảo mật của các gói được trao đổi, và cơ chế chống phát lại. | Tất cả các đảm bảo an ninh được thực hiện qua TLS 1.2 với mật mã TLS sau các bộ xác định tất cả các nguyên hàm điện tử: thiết bị camera hoạt động như máy chủ TLS cung cấp các bộ mật mã sau đây dành cho thiết lập kết nối: ECDHE-ECDSA-AES128-GCM-SHA256 hoặc ECDHE-ECDSA-AES256-GCM-SHA384. | Kết nối sử dụng TLS được xác định rõ giao thức để thiết lập kết nối, trong đó bao gồm một chuỗi giao thức được sắp xếp, được xác định máy trạng thái, khởi tạo và xác định cơ chế thiết lập lại. Kết nối lại hàng loạt có thể dẫn đến DoS của thiết bị camera, tuy nhiên tính bảo mật của các dịch vụ của nó sẽ không bị ảnh hưởng. |

**Bảng C.12 - Mẫu IXIT 12-NetSecImpl (Bảo mật đường truyền mạng)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Mô tả** | **Phương pháp thực hiện** | **Báo cáo** |
| NetSecImpl-1 | Chức năng mạng làđược triển khai bởi hệ điều hành Linux. Mục đích của nó là cung cấp API để sử dụng như máy chủ web nội bộ. Nó là một phần của Linux kernel, phiên bản 5.10.30. | Hệ điều hành Linux được sử dụng rộng rãi trên tất cả các loại hệ thống trên toàn thế giới. Bản thân Nhà cung cấp đã không xem xét. Nó tin tưởng vào phân tích được thực hiện bởi các nhà nghiên cứu bảo mật không được tuyển dụngVí dụ báo cáo lỗi được mô tả trên các trang web của Linux Foundation | Không có gì được tạo ra đặc biệt cho thiết bị camera này. |

**Bảng C.13: Mẫu IXIT 13-SoftServ (Dịch vụ phần mềm)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Trạng thái (Bật/Tắt)** | **Giải thích** | **Cho phép cấu hình (Có/Không)** | **Cơ chế xác thực** |
| SoftServ-1 | Dịch vụ web cung cấp giao diện. Dịch vụ này có thể truy cập được qua mạng. Dịch vụ này có thể truy cập được trong trạng thái khởi tạo. | Đã bật | Dịch vụ này là cần thiết để cung cấp cho người dùng khả năng cấu hình thiết bị camera. | Đúng. Người dùng có thể• cấu hình tên người dùng/mật khẩu để truy cập web• cấu hình tài khoản SSH. | AuthMech-1,AuthMech-2 |

**Bảng C.14: Mẫu IXIT 14-SecMgmt (Quy trình quản lý bảo mật)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| SecMgmt-1 | Nhà cung cấp sử dụng ANSI/ISA-62443 để quản lý các quy trình quản lý bảo mật của mình. Điều này bao gồm tất cả các tham số bảo mật quan trọng được liệt kê trong IXIT 10-SecParam. Tài liệu hướng dẫn thực hiện tiêu chuẩn được đính kèm. Để phù hợp với tiêu chuẩn, nó bao gồm việc tạo và cung cấp các tham số bảo mật theo phần 5 và 8. Việc lưu trữ được thực hiện theo phần 5. Các bản cập nhật được xử lý theo phần 9, 10 và 11. Việc ngừng hoạt động và hết hạn thiết bị camera được thực hiện theo mục 12. |

**Bảng C.15: Mẫu IXIT 15-Intf (Giao diện)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Loại** | **Tình trạng (Kích hoạt/Không kích hoạt)** | **Thông tin có thể tiết lộ** | **Giao diện gỡ lỗi** | **Biện pháp bảo vệ** |
| Intf-1 | Giao diện Ethernet cần thiết để cấu hình thiết bị camera. | Mạng | Đã kích hoạt, vì người dùng cần truy cập vào để cấu hình thiết bị camera. | Giao diện này tiết lộ số hiệu phiên bản máy chủ web Apache. Thông tin này có liên quan đến bảo mật bởi vì nó có thể đưa ra gợi ý cho kẻ tấn công về CVE mà thiết bị camera dễ bị tổn thương. | Không áp dụng(Không gỡ lỗi) | Không áp dụng(Không phải giao diện vật lý) |

**Bảng C.16: Mẫu IXIT 16-CodeMin (Tối ưu mã nguồn)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| CodeMin-1 | Mã được phân tích bằng các công cụ phân tích mã tĩnh trong giai đoạn phát triển. Các công cụ liệt kê các chức năng không sử dụng sẽ bị loại bỏ theo mục 8 của ANSI/ISA-62443. |

**Bảng C.17: Mẫu IXIT 17-PrivlCtrl (Kiểm soát phân quyền)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| PrivlCtrl-1 | Nhà cung cấp sử dụng quy trình thiết kế mã an toàn theo mục 7 của ANSI/ISA-62443. Điều này bao gồm mỗi thành phần của thiết bị camera một danh sách của tất cả các tài khoản người dùng kỹ thuật và đặc quyền của họ được duy trì. Trong quá trình thiết kế, các đặc quyền được lên kế hoạch để có cấu hình tối thiểu sao cho hoạt động của thiết bị camera không bị xáo trộn. Sau đó, việc triển khai đúng các đặc quyền đã xác định sẽ được kiểm tra bằng các thử nghiệm theo mục 9 của ANSI/ISA-62443 để đảm bảo rằng mỗi thành phần đang hoạt động với ít nhất các đặc quyền có thể. |

**Bảng C.18: Mẫu IXIT 18-AccCtrl (Kiểm soát truy cập)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| AccCtrl-1 | Thiết bị camera sử dụng bộ xử lý ARM Cortex A8 bao gồm bộ phận quản lý bộ nhớ chịu trách nhiệm chỉ định quyền truy cập bộ nhớ và bộ nhớ thuộc tính cho các vùng riêng biệt cho các quy trình khác nhau. Đơn vị quản lý bộ nhớ điều khiển phần cứng đi theo bảng truy cập vào các bảng dịch trong bộ nhớ bằng cách cho phép điều khiển hệ thống bộ nhớ chi tiết thông qua một tập hợp các ánh xạ địa chỉ ảo đến vật lý và các thuộc tính bộ nhớ được giữ trong lệnh và dữ liệu. Hệ điều hành Arch Linux® ARM phụ thuộc rất nhiều vào việc sử dụng đơn vị quản lý bộ nhớ, đặc biệt là quản lý bảng trang của nó. |

**Bảng C.19: Mẫu IXIT 19-SecDev (Quy trình phát triển phần mềm an toàn)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| SecDev-1 | Nhà cung cấp sử dụng quy trình phát triển an toàn theo ANSI/ISA-62443. Điều này bao gồm đặc điểm kỹ thuật của các yêu cầu bảo mật theo mối đe dọa, quy trình xem xét được xác định bởi ít nhất hai người về thiết kế bảo mật, việc sử dụng tiêu chuẩn mã hóa MISRA-C để triển khai đúng định dạng trình bày, ứng dụng lập trình cặp sao cho mọi thay đổi mã đều được xem xét bởi ít nhất một người bổ sung và các chiến lược thử nghiệm được xác định. |

**Bảng C.20: Mẫu IXIT 20-SecBoot (Cơ chế khởi động thiết bị an toàn)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Điều kiện bảo đảm bảo mật** | **Cơ chế phát hiện vi phạm** | **Thông báo cho người dùng** | **Chức năng thông báo** |
| SecBoot-1 | Thiết bị camera thực hiện quy trình khởi động an toàn. Bộ khởi động dựa trên Trusted Board Boot (TBB), ngăn chặn phần mềm độc hại chạy trên nền tảng bằng cách xác thực tất cả các hình ảnh firmware đến và bao gồm cả bộ khởi động thế giới bình thường. Điều này được thực hiện bằng cách thiết lập một Chuỗi Tin cậy sử dụng các Tiêu chuẩn Mã hóa Công khai (PKCS). Gốc của sự tin cậy là một khóa công khai được mã hóa cứng và được tải lần đầu tiên tại cấu hình thiết bị camera. Khóa tin cậy là không thể thay đổi và không thể thay đổi. Gốc của sự tin cậy cùng với chip RAM được chứng nhận theo cấp độ PSA 3. Một giá trị SHA256 của khóa này được lưu trữ vào các thanh ghi khóa gốc tin cậy. Cơ chế khởi động bao gồm nhiều bộ khởi động. "Bộ khởi động 1" (BL1) nằm trong ROM nên không thể bị sửa đổi. Các hình ảnh bộ khởi động kế tiếp BL2, BL31 và BL33 được tải lần lượt, trong đó mỗi BL sẽ được xác thực tính toàn vẹn bởi BL trước đó. Một chuỗi tin cậy cho phần mềm được tải bởi chip ARM được thực hiện như mô tả trong phần "Chuỗi Khởi động Tin cậy" tại <https://github.com/ARM/software/arm-trusted-firmware/blob/master/docs/design/trusted-board-boot.rst>. | Bằng cách thiết lập một chuỗi tin cậy nhất quán, toàn bộ hình ảnh phần mềm, bao gồm cả nhân hệ điều hành, được bảo vệ, đảm bảo cả tính toàn vẹn và tính xác thực. Hình ảnh phần mềm được bảo vệ chống lại sự thao túng trước khi khởi động. | Nếu một phần bất kỳ của chuỗi bộ khởi động, bao gồm hình ảnh phần mềm, không thể được xác thực, quá trình xác minh bộ khởi động của thiết bị camera sẽ thất bại vì kiểm tra chữ ký không thành công. Trong trường hợp này, thiết bị camera sẽ gặp lỗi và dừng hoàn toàn quá trình khởi động. | Người dùng sẽ được thông báo qua đèn LED nhấp nháy màu đỏ ở bên trái của thiết bị camera khi có sự thay đổi không được phép. | Không liên quan tới chức năng mạng nào. |

**Bảng C.21: Mẫu IXIT 21-PersData (Dữ liệu cá nhân)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Hành động** | **Cơ chế kết nối** | **Tính nhạy cảm****(Có/Không)** | **Thu thập sự đồng ý** | **Rút lại sự đồng ý** |
| PersData-1 | Tên đầy đủ của người dùng | Tên người dùng được nhập trên ứng dụng hoặc giao diện web và được sử dụng cho thông báo. Ngoài ra tên người dùng sẽ được sử dụng để cung cấp kèm theo báo cáo lỗi cho Nhà cung cấp. | ComMech-2, ComMech-1. | Có | Người dùng cần xác nhận điều khoản và điều kiện chung trước khi cài đặt thiết bị camera và ứng dụng. | Người dùng có thể rút lại sự đồng ý bằng cách đặt lại thiết bị camera thành mặc định của nhà máy. |

**Bảng C.22: Mẫu IXIT 22-ExtSens (Cảm biến bên ngoài)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| ExtSens-1 | Microphone để ghi lại âm thanh môi trường của thiết bị camera nằm ở mặt trước của thiết bị camera. |
| ExtSens-2 | Camera (quang phổ nhìn thấy được) để ghi lại môi trường của thiết bị camera nằm ở mặt trước của thiết bị camera. |
| ExtSens-3 | Camera (phổ hồng ngoại) dành cho chức năng cảm biến chuyển động của thiết bị camera nằm ở mặt trước của thiết bị camera. |

**Bảng C.23: Mẫu IXIT 23-ResMech (Cơ chế khôi phục sau sự cố)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Mô tả** | **Loại** | **Điều kiện bảo đảm bảo mật** |
| ResMech-1 | Thiết bị camera sử dụng pin tích hợp có thể cung cấp năng lượng cho thiết bị camera trong 15 phút. Sau 12 phút mất điện, thiết bị camera sẽ bắt đầu quy trình tắt máy an toàn. | Mất điện | Các chức năng chính của thiết bị camera, phát video và âm thanh, hoàn toàn duy trì hoạt động nếu mất điện tối đa 12 phút.Trong trường hợp mất điện đột ngột, thiết bị camera vẫn hoạt động sau khi khởi động lại và không bị ảnh hưởng tiêu cực bởi hệ thống tập tin bị hỏng. |

**Bảng C.24: Mẫu IXIT 24-TelData (Dữ liệu đo đạc từ xa)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Mục đích** | **Kiểm tra an ninh** | **Dữ liệu cá nhân** |
| TelData-1 | Dữ liệu sự cố trong trường hợp lỗi dịch vụ. Trong trường hợp quy trình bị lỗi, thiết bị camera lưu lại một tệp kết xuất lõi chứa trạng thái của một quá trình khi quá trình nhận được một số phản hồi nhất định. Tệp kết xuất bao gồm ảnh chụp nhanh của bộ nhớ được phân bổ và các tiến trình. | Dữ liệu sẽ được phân tích bằng Nhà cung cấp để cải thiện đặc biệt là tính ổn định của hệ thống sản phẩm của mình. | Dữ liệu đo từ xa được tải lên sau sự cố (gây ra do vi phạm bảo mật) mà không có bất kỳ sự tương tác nào của người dùng với các dịch vụ liên quan (cơ sở hạ tầng đám mây) của Nhà cung cấp để có thể phân tích những gìgây ra sự cố và những cải tiến về mãkhả thi. Kết xuất lõi được phân tích bằng GDB và các công cụ tương tự do nhân viên của Nhà cung cấp thực hiện để đạt được những thông tin cần thiết. | PersData-3,PersData-4,PersData-5 |

**Bảng C.25: Mẫu IXIT 25-DelFunc (Chức năng hủy bỏ và khôi phục cài đặt gốc)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Mô tả** | **Đối tượng** | **Khởi tạo và tương tác** | **Xác nhận** |
| DelFunc-1 | Người dùng có thể chọn đặt lại thiết bị camera về trạng thái ban đầu mặc định. Trong trường hợp này tất cả dữ liệu cấu hình được tạo bởi người dùng hoặc được tạo ra do người dùng cung cấp đầu vào sẽ bị xóa khỏi bộ nhớ flash.Tất cả dữ liệu cấu hình được tạo trong định nghĩa tập tin cấu hình (cơ sở dữ liệu SQLite) bị xóa khỏi hệ thống tập tin trong bộ nhớ flash. Sau đó mới tập tin cấu hình được tạo với nội dung trống. | Dữ liệu người dùng trên thiết bị | Người dùng cần chọn "Bảo trì" -> "Đặt lại" trên giao diện web hoặc "Bảo trì" -> "Đặt lại" trong ứng dụng. | Trước khi bắt đầu xóa ứng dụng hoặc giao diện web đưa ra thông báo về quá trình xóa và thông báo cho người dùng về lần khởi động lại tiếp theo. Sau đó xóa thiết bị camera được khởi động lại và ở chế độ mặc định của nhà sản xuất. Người dùng có thể xác minh điều này bằng cách nhận thấy rằng thiết bị camera không còn được kết nối với Mạng không dây và người dùng không thể truy cập giao diện trong mạng.. |

**Bảng C.26: Mẫu IXIT 26-UserDec (Tương tác của người dùng)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Mô tả** | **Tùy chọn** | **Kích hoạt (Có/Không)** |
| UserDec-1 | Người dùng cần đặt mật khẩu mới cho người dùng quản trị. Đây là hành động đầu tiên người cần thực hiện để thiết lập thiết bị camera. | Người dùng cần chọn mật khẩu phù hợp với các quy tắc mật khẩu. Độ an toàn của mật khẩu đã chọn sẽ được hiển thị cho người dùng. | Người dùng muốn truy cập thiết bị camera thông qua ứng dụng hoặc web giao diện lần đầu tiên. Quyết định không thể được kích hoạt bởi người dùng. |

**Bảng C.27: Mẫu IXIT 27-UserIntf (Giao diện người dùng)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| UserIntf-1 | Người dùng có thể nhập dữ liệu cấu hình trên giao diện web có thể truy cập trên cổng từ xa 443. |

**Bảng C.28: Mẫu IXIT 28-ExtAPI (Dịch vụ liên kết)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| ExtAPI-1 | Thiết bị camera cung cấp giao diện SOAP có thể được các thiết bị khác sử dụng để điều khiển chuyển động của thiết bị camera và nhận các luồng âm thanh và video thông qua một kết nối trực tiếp trên cổng từ xa 8085. |

**Bảng C.29 Mẫu IXIT 29-InpVal (Kiểm tra dữ liệu đầu vào)**

|  |  |
| --- | --- |
| **ID** | **Mô tả** |
| InpVal-1 | Đối với mỗi dữ liệu người dùng được truyền tới thiết bị camera qua một trong các API của nó, quy tắc xác thực đã xác định sẽ được áp dụng. Quy tắc xác thực bao gồm ít nhất một biểu thức chính quy nhận dữ liệu đầu vào và trả về xem đầu vào có khớp với biểu thức hay không. Trong trường hợp đầu vào phức tạp hơn, đầu vào có thể được so khớp với không chỉ một mà là một tập hợp các biểu thức chính quy để thiết bị camera chỉ xử lý các giá trị hợp lệ. Các giá trị không hợp lệ sẽ bị từ chối.Biểu thức chính quy được áp dụng trên mọi dữ liệu nhận được từ giao diện web, giao diện SOAP và ứng dụng. |

PHỤ LỤC C

**(Quy định)**

**Mã HS thiết bị camera giám sát sử dụng giao thức Internet**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên sản phẩm, hàng hóa theo QCVN** | **Mã số HS** | **Mô tả sản phẩm, hàng hóa** |
| **1** | Thiết bị camera giám sát sử dụng giao thức Internet | 8525.60.008525.81.108525.81.908525.82.108525.82.908525.83.108525.83.908525.89.108525.89.90 | Camera kỹ thuật số, có thể kết nối qua giao thức Internet thực hiện một phần hoặc toàn bộ việc giám sát, ghi hình. |