TECNOLOGÍAS DE LA INFORMACIÓN Y CIBERSEGURIDAD

Proyecto aplicado a seguridad en Domótica

Proyecto para optar al grado de Ingeniero/Licenciado en Ciberseguridad

Asignatura: Seminario de grado

Sección: 7101D

Nombre del profesor guía: Felipe Arancibia B.

Nombre de los estudiantes: Victor Jaramillo Rute.

Hernán Urtubia Baeza.

Elgart Yáñez Hernández.

Nicolás Cornejo Fernández.

Fecha de entrega

09 de noviembre de 2023.

Contenido

Introducción

Como se ha ido hablando a lo largo de este proyecto, el uso de la domótica en hogares es cada vez más común, lo cual ha generado nuevas amenazas al hogar, esto debido a que los ciberdelincuentes aprovechan la poca seguridad con la que se cuenta en estos sistemas para poder espiar y recolectar información de las personas que habitan los hogares, para esto se usa las cámaras IP, que funcionan como motores de búsqueda de dispositivos conectados a internet y, por ende, permiten ver cámaras IP que no cuentan con los niveles de seguridad mínimos para no ser expuestas, una de las páginas más reconocidas es Shodan[.]io, la cual es uno de los motores de búsqueda y escáner de dispositivos y sistemas en Internet..

Para ayudar a los usuarios a tener un mejor nivel de seguridad en sus cámaras IP, se propone como solución, la creación de un manual de buenas prácticas para cámaras IP. En este manual se busca educar al usuario, enseñándole cuales son las medidas de seguridad más básicas que se pueden aplicar y como implementarlas.

En el siguiente informe se tratará sobre el método para recolectar la información, en este caso se usará una encuesta que permitirá saber el estado actual en el que se encuentran los usuarios en cuanto a conocimientos de la seguridad informática que abarca a sus dispositivos y permitirán confirmar la problemática previamente planteada, también se aplicarán las matrices de riesgos e inventario de activos necesarios, este última detalla los activos presentes en un sistema de cámaras IP convencional hoy por hoy, en el cual se pueden ver las cámaras a través de una app móvil y/o un servidor web. Para finalizar, se hablará sobre el método de validación, el cual permitirá validar la hipótesis propuesta, demostrando que la solución es válida.

Técnicas de Recopilación de Información

Para la recolección de datos, se usará una encuesta elaborada en formularios de Google, esta contar con un total de 10 preguntas, las cuales estarán enfocada en acciones que puede tomar el usuario y también en conocer aspectos básicos de su sistema de cámaras, por ejemplo, cantidad de cámaras que usa o marca y modelo de estas. En la encuesta no se realizarán preguntas técnicas ni se usará un lenguaje técnico, debido a que esta encuesta está dirigida a usuarios particulares de cámaras IP, por lo que no necesariamente deben tener conocimiento técnico sobre el manejo de cámaras. Se espera encuestar a un total de 25 usuarios de cámaras, con los cuales, no se tendrá en cuenta su rango etario u ocupación laboral.

El uso de esta encuesta tiene como objetivo comprender de mejor manera el conocimiento actual con el que cuentan los usuarios de cámaras IP, así pudiendo confirmar que el problema planteado es verídico. Se espera al momento de analizar la información, se rebele que los usuarios no tienen conocimientos sobre la seguridad que se aplica a sus cámaras, por lo que no contaran con ninguna medida, como el cambio de contraseña o el control de la conexión remota a la cámara, entre otras medidas.

Las preguntas que se usarán en la encuesta son la siguiente

¿ Tiene conocimientos sobre ciberseguridad ? *

- ◯ Si
- ◯ No

¿Estás al tanto de los riesgos de seguridad asociados con las cámaras IP? *

- ◯ Si
- ◯ No

¿Ha cambiado la contraseña predeterminada de su cámara IP? *

- ◯ Si
- ◯ No

¿Cada cuanto tiempo cambia la contraseña de usuario para ingresar a su cámara IP? *

- ◯ 3 meses
- ◯ 6 meses
- ◯ 1 año
- ◯ Nunca

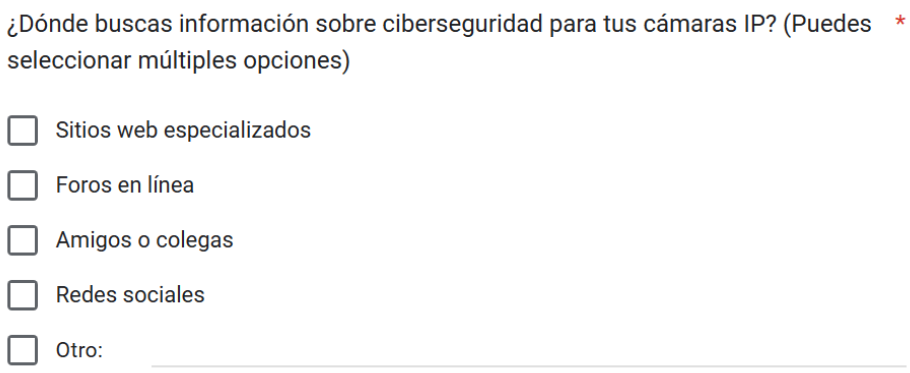

Imagen 1: Encuesta conocimiento de seguridad

Fuente: Elaboración propia (https://docs.google.com/forms/d/e/1FAIpQLSf5Gxk1rP_jwsxLztG9uWwD97eLVXA1V9NeTQqjGDhjALEFIg/viewform?usp=sf_link)

Identificación de Activos

Tabla 1: Matriz de Activos

Activo	Clasificación	Ubicación
Router Hogar	Físico	Casa del usuario
Cámara IP YOOSEE	Físico	Casa del usuario
Cámara IP Smart Net	Físico	Casa del usuario
Aplicación móvil	Lógico	Smartphone
Servidor de almacenamiento en la nube y acceso remoto a cámaras	Lógico	Datacenter de la empresa proveedora del servicio de CCTV
Computador (Escritorio o laptop)	Físico	Casa del usuario
Smartphone personal del cliente	Físico	Casa del usuario

Fuente: Elaboración Propia

Matriz de Riesgos

Tabla 2: Matriz de Riesgos de cámaras IP

AMENAZA	VULNERABILIDAD	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS	ROBABILIDA	IMPACTO	RIESGO	D RIESGO
Espionaje remoto	Contraseñas de cámaras IP por defecto	El o los atacantes realiza espionaje remoto de la información íntima de las personas registradas por las cámaras IP domésticas, con fines extorsivos, aprovechando que mantienen su contraseña de fábrica	Pérdidas económicas por exigencias de naturaleza extorsiva de los criminales para no revelar información íntima de las personas	3	3	9	R1
	Contraseñas de sitio web de acceso a la cámara por defecto o igual al de la cámara IP con contraseña por defecto	El o los atacantes realizan espionaje remoto de la información íntima de las personas registradas por cámaras IP domésticas, con fines de extorsión, aprovechando que mantienen su contraseña por defecto		3	3	9	R2
Escucha encubierta	Tráfico sensible sin protección	Falta de cifrado en los datos enviados que impida que se extraiga información sensible del usuario (contraseñas, cuentas de correo). Un atacante puede acceder al dispositivo sin tener limitaciones pasando desapercibido.	Daño a la reputación de los dueños de las cámaras IP por invasión de su intimidad	2	2	4	R3
		Permite a atacantes remotos descubrir las contraseñas a través de un paquete de transmisión UDP.	Manipulación indebida de las credenciales de la cámara IP por parte de un atacante	2	2	4	R4
			Pérdida reputacional del fabricante	1	2	2	R5
Denegación de servicio distribuida (DDoS)	Contraseñas de cámaras IP por defecto	Incriminación de los dueños de las cámaras en un ataque de Denegación distribuida del servicio de páginas de terceros a través del uso de sus cámaras aprovechando que mantienen su contraseña de fábrica.	Posibles problemas legales y afectación de la reputación del (los) dueños de las cámaras IP reclutadas para la botnet.	2	3	6	R6
		Denegación distribuida del servicio a páginas de terceros a través del uso de cámaras IP como parte de una Botnet aprovechando la contraseña por	Ingresos no percibidos por ventas de bienes y servicios no realizadas	2	3	6	R7
Error del usuario	Falta de conciencia de seguridad	Exposición a ciberataques al no leer los manuales de usuario de las cámaras IP y no seguir buenas prácticas de seguridad.	Sustracción y/o pérdida de la información resguardada en las cámaras IP	3	3	9	R8
	Autenticación débil	Exposición a ataques de fuerza bruta y diccionario permitiendo que un atacante descifre las claves de acceso.	Pérdidas económicas por extorsión de los atacantes para no revelar información íntima de las personas.	3	3	9	R9
Interceptación de señales	Falta de cifrado en datos enviados a través de la red (contraseñas e imágenes de la grabación en tiempo real)	Exposición de sniffing ocasionando que un atacante pueda tener conocimiento de información susceptible para el usuario.	Daño a la reputación del (los) dueño/s de las cámaras IP, al compartir la información íntima de las personas a terceros.	2	2	4	R10
Datos provenientes de fuentes no confiables	Inyección de código	Permite que un atacante pueda realizar la carga de archivos que intenta modificar ficheros y valores de la estructura funcional del dispositivo para llevar a cabo ataques y comprometer la seguridad y privacidad de los usuarios	Pérdida económica por extorsión de los atacantes para no revelar información íntima de las personas.	1	3	3	R11
Manipulación con software	Descarga y uso no controlado de software	Realizar el acceso a las funciones de la cámara a través de software no autorizado por el fabricante que permita que la información y configuración de la cámara queden expuestos a terceros.	Daño a la reputación del (los) dueño/s de las cámaras IP, al exponer la información almacaenada en ellas.	2	3	6	R12
Uso de software no legítimo	No verificar la autenticidad del sitio web al que se accede para ingresar a las funciones de la cámara.	Exposición a Phising permitiendo la captura de información sensible del usuario (cuentas de correo, contraseñas, ubicación del dispositivo)	Daño a la reputación del (los) dueño/s de las cámaras IP por exponer la información del usuario.	2	3	6	R13
Uso no autorizado de la cámara	Acceso de forma remota sin autenticación	Permite a los atacantes remotos obtener acceso administrativo a través de una sesión TELNET que les permite conocer la información ingresada requerida para la configuración inicial (cuentas de correo, ubicación del dispositivo, números de contacto, contraseñas), así como poder acceder a la transmisión en tiempo real.	Daño a la reputación del (los) dueño/s de las cámaras IP por invasión de la intimidad sin consentimiento del usuario.	1	2	2	R14
	Falta de autenticación robusta	Se puede ver afectada la confidencialidad de la información por acceso de terceros para realizar manipulación del dispositivo.	Posibles pérdidas económicas debido a la manipulación de la cámara por parte de terceros.	2	3	6	R15

Fallas de la cámara	Falta de mantenimiento preventivo	Compromiso de disponibilidad de las grabaciones	Pérdida parcial o total de las grabaciones	3	3	9	R16
	Firmware desactualizado	Daño de hardware provocado por virus informático	Posible daño funcional de la cámara IP	3	3	9	R17
	Acceso de forma remota sin autenticación	Vulnerabilidades propias de los fabricantes	Perdida reputacional del fabricante	1	2	2	R18
		Al explotar la vulnerabilidad presentada en las cámaras, un atacante puede llegar a tener información valiosa propia del dispositivo al ubicarse en el archivo de configuración de forma remota a través de la ruta <camera-IP> /common/info.cgi, esto sin requerir autenticación previa.	Perdida reputacional del fabricante al tener acceso de la información propia de la cámara (modelo, producto, marca, versión, compilación, nombre del dispositivo, ubicación, dirección MAC, dirección IP, estado inalámbrico)	1	2	2	R19
	Errores de fabricación	Credenciales débiles para el acceso a la interfaz web administrativa del fabricante, permite que un usuario malintencionado obtenga acceso no autorizado a archivos CGI y pueda modificar información esencial para el funcionamiento de la cámara.	Posibles pérdidas económicas que genere el daño del dispositivo por modificación en los parámetros de funcionamiento establecidos por el fabricante.	1	2	2	R20
Hurto del dispositivo	Ausencia de protección física	Compromiso de disponibilidad de la información por robo del dispositivo	Pérdida de las grabaciones	2	3	6	R21
		Compromiso de la confidencialidad de la información por la pérdida de las grabaciones almacenadas en el dispositivo	Pérdidas económicas al presentarse el hurto de las cámaras	2	2	4	R22
			Pérdidas económicas por extorsión de los criminales para no revelar información privada de las personas.	2	3	6	R23
Falla en las telecomunicaciones de la cámara	Conexión deficiente de la comunicación	Se puede ver afectada la disponibilidad de las grabaciones del dispositivo en un determinado rango de tiempo	Pérdida de las grabaciones	2	1	2	R24
	Conexiones de red sin protección	Impedimento del acceso remoto autorizado a la configuración de la cámara	El usuario no podrá modificar ninguna función de la cámara durante el tiempo que dure la falla	2	1	2	R25
		Exposición a ataques "Man in the Middle" interceptando información transmitida en la red (direcciones IP, credenciales, imágenes en tiempo real, cuentas de correo)	Pérdidas económicas por extorsión de los atacantes para no revelar información íntima de las personas.	2	2	4	R26
Daños o destrucción de la cámara	Ubicación vulnerable del dispositivo	Pérdida total o parcial de la información por acceso a la propiedad de un intruso	Pérdidas económicas para el usuario por la destrucción de la cámara por parte de criminales o por actos de vandalismo	1	3	3	R27
Pérdida de suministro eléctrico	Funcionamiento inadecuado del suministro eléctrico	Pérdida parcial de la grabación en tiempo real al no tener continuidad en el servicio de energía	Posibles pérdidas económicas por variaciones de voltaje de energía que impacten el funcionamiento de la cámara de acuerdo a las recomendaciones del fabricante	1	2	2	R28
Fuego, agua y polvo	Susceptibilidad a la humedad, polvo y fuego	Indisponibilidad de la información por fallas en la grabación generando pérdida parcial o total de la información	Pérdidas económicas por fallas en el funcionamiento de la cámara derivadas de condiciones ambientales	2	1	2	R29

Fuente: Universidad católica de Colombia, Facultad de ingeniería, identificación de riesgos en la seguridad de la información de cámaras de vigilancia domésticas en entornos IOT.

Técnicas de Validación

Para el desarrollo y ejecución del proyecto, existen varias técnicas y métodos que son útiles para la validación de la hipótesis de que el uso de un manual de buenas prácticas para cámaras IP aumenta la seguridad de los usuarios. Entre dichas técnicas se encuentran: Análisis de casos de estudio, Comparativa antes y después de lectura, datos de adopción y uso de cámaras IP, entrevistas a expertos en el tema, estadística de ciberataques, evaluación de tendencias de seguridad y encestas o cuestionarios respecto al tema. En el caso del proyecto actual la técnica de validación a utilizar será la encuesta o cuestionario respecto al tema, dicha encuesta será dirigida a los usuarios del manual para cuantificar los resultados respecto al cambio de percepción, comprensión y conocimiento por parte de los usuarios.

Dentro de dicho cuestionario se encontrarán preguntas de relevancia como:

¿Cada cuánto tiempo se debería cambiar la contraseña de usuario para ingresar a su cámara IP?

Esta pregunta está asociada a la comprensión lectora del usuario tras la lectura del manual, en búsqueda de una mejoría en cuanto al manejo de las claves por parte del usuario, la respuesta a esta pregunta será en base a los lapsos que se establecerán en el manual.

¿Cuáles son los riesgos ante el uso de una cámara IP?

Esta es una pregunta asociada a los riesgos que se mencionaran en el manual de buenas prácticas, la respuesta que se busca obtener será un ejemplo de los riesgos y/o ataques que se dan a conocer en el manual.

¿Siente usted que el manual le ayudo a comprender de mejor forma la ciberseguridad en cuanto a cámaras IP?

La pregunta funcionara como método de satisfacción para el usuario tras la lectura y comprensión del manual de buenas prácticas, a su vez se busca el obtener una retroalimentación de parte del usuario para futuras versiones del manual.

Como método para validar la hipótesis del presente proyecto se citan las siguientes vulnerabilidades reportadas para cámaras IP desde el año 2021 hasta la fecha, esto con el objetivo de visualizar los vectores explotados por intrusos y/o atacantes:

- ***CVE-2021-1131:*** Una vulnerabilidad en la implementación del protocolo Cisco Discovery para las cámaras IP de la serie 8000 de vigilancia por vídeo de Cisco podría permitir a un atacante adyacente no autenticado provocar la recarga de una cámara IP afectada. La vulnerabilidad se debe a la falta de comprobaciones cuando se procesan los mensajes de Cisco Discovery Protocol. Un atacante podría aprovechar esta vulnerabilidad mediante el envío de un paquete malicioso Cisco Discovery Protocol a una cámara IP afectada. Un ataque exitoso podría permitir al atacante hacer que la cámara IP afectada se recargue inesperadamente, dando lugar a una denegación de servicio (DoS). Nota: Cisco Discovery Protocol es un protocolo de Capa 2. Para explotar esta vulnerabilidad, un atacante debe estar en el mismo dominio de difusión que el dispositivo afectado (Capa 2 adyacente).

- ***CVE-2021-1521:*** Una vulnerabilidad en la implementación del protocolo Cisco Discovery para las cámaras IP de la serie 8000 de vigilancia por vídeo de Cisco podría permitir a un atacante adyacente no autenticado provocar la recarga de una cámara IP afectada. Esta vulnerabilidad se debe a la falta de comprobaciones al procesar los mensajes de Cisco Discovery Protocol. Un atacante podría explotar esta vulnerabilidad mediante el envío de un paquete malicioso Cisco Discovery Protocol a una cámara IP afectada. Un ataque exitoso podría permitir al atacante hacer que la cámara IP afectada se recargue inesperadamente, dando lugar a una denegación de servicio (DoS). Nota: Cisco Discovery Protocol es un protocolo de Capa 2. Para explotar esta vulnerabilidad, un atacante debe estar en el mismo dominio de difusión que el dispositivo afectado (Capa 2 adyacente).

- ***CVE-2021-23847***: La falta de autenticación en una función crítica de las cámaras IP de Bosch permite a un atacante remoto no autenticado extraer información confidencial o cambiar la configuración de la cámara enviando solicitudes falsificadas al dispositivo. Sólo los dispositivos de la familia CPP6, CPP7 y CPP7.3 con firmware 7.70, 7.72 y 7.80 anteriores a B128 están afectados por esta vulnerabilidad. Las versiones 7.62 o inferiores y las cámaras INTEOX no están afectadas.

- ***CVE-2021-23848:*** Un error en el manejador de URL de las cámaras IP de Bosch puede provocar un cross site scripting (XSS) reflejado en la interfaz basada en web. Un atacante con conocimiento de la dirección de la cámara puede enviar un enlace crafteado a un usuario, que ejecutará código javascript en el contexto del usuario.

- ***CVE-2021-23850:*** Un paquete TCP/IP especialmente diseñado puede provocar el bloqueo de la interfaz telnet de una imagen de recuperación de cámara. También puede causar un desbordamiento de búfer que podría permitir la ejecución remota de código. La imagen de recuperación sólo puede arrancarse con derechos administrativos o con acceso físico a la cámara y permite cargar un nuevo firmware en caso de firmware dañado.

- ***CVE-2021-23851:*** Un paquete TCP/IP especialmente diseñado puede provocar el bloqueo de la interfaz web de recuperación de imágenes de la cámara. También puede causar un desbordamiento de búfer que podría permitir la ejecución remota de código. La imagen de recuperación sólo se puede arrancar con derechos administrativos o con acceso físico a la cámara y permite cargar un nuevo firmware en caso de firmware dañado.

- ***CVE-2021-23852:*** Un atacante autenticado con derechos de administrador de cámaras IP Bosch puede llamar a una URL con un parámetro no válido que hace que la cámara deje de responder durante unos segundos y provoque una denegación de servicio (DoS).

- ***CVE-2021-26611:*** La cámara IP HejHome GKW-IC052 contiene una vulnerabilidad de credenciales codificadas. Este problema permite a atacantes remotos operar la cámara IP (reinicio, restablecimiento de fábrica, instantánea, etc.).

- ***CVE-2021-30166:*** La función de configuración del servidor NTP del dispositivo de cámara IP no se verifica con parámetros especiales. Los atacantes remotos pueden realizar un ataque de inyección de comandos y ejecutar comandos arbitrarios después de iniciar sesión con el permiso privilegiado.

- ***CVE-2021-4045:*** La cámara IP TP-Link Tapo C200, en su versión de firmware 1.1.15 e inferiores, está afectada por una vulnerabilidad RCE no autenticada, presente en el binario uhttpd que se ejecuta por defecto como root. La explotación de esta vulnerabilidad permite a un atacante tomar el control total de la cámara.

- ***CVE-2021-41506:*** Xiaongmai

    1. AHB7008T-MH-V2
    2. AHB7804R-ELS
    3. AHB7804R-LMS
    4. AHB7804R-MH-V2
    5. AHB7808R-MS
    6. AHB7808R-MS-V2
    7. AHB7808T-MS-V2
    8. HI3518_50H10L_S39
    9. V4.02.R11.7601.Nat.Onvif.20170420
    10. V4.02.R11.Nat.Onvif.20160422
    11. V4.02.R11.7601.Nat.Onvif.20170424
    12. V4.02.R11.Nat.Onvif.20170327
    13. V4.02.R11.Nat.20170301
    14. V4.02.R12.Nat.OnvifS.20170727

    Están afectados por un backdoor en los binarios macGuarder y dvrHelper del firmware de la cámara DVR/NVR/IP debido a las credenciales estáticas de la cuenta root en el sistema.

- ***CVE-2021-45039***: Varios modelos de la cámara IP Uniview (por ejemplo, IPC_G6103 B6103.16.10.B25.201218, IPC_G61, IPC21, IPC23, IPC32, IPC36, IPC62 e IPC_HCMN) ofrecen un servicio UDP no documentado en el puerto 7788 que permite a un atacante remoto no autenticado desbordar un búfer interno y lograr la ejecución de código. Utilizando este desbordamiento de búfer, un atacante remoto puede iniciar el servicio telnetd. Este servicio tiene un nombre de usuario y contraseña predeterminados (root/123456). Aunque tiene un shell restrictivo, esto puede ser fácilmente evitado a través del comando shell ECHO incorporado.

- ***CVE-2022-23382:*** Shenzhen Hichip Vision Technology IP Camera Firmware V11.4.8.1.1-20170926 tiene una vulnerabilidad de denegación de servicio a través del envío de un mensaje multicast elaborado en una red local.

- ***CVE-2022-28743:*** La vulnerabilidad Race Condition de Time-of-check Time-of-use (TOCTOU) en la cámara IP Foscam R2C que ejecuta System FW <= 1.13.1.6, y Application FW <= 2.91.2.66, permite a un atacante remoto autenticado con permisos de administrador ejecutar código remoto arbitrario a través de un parche de firmware malicioso. El impacto de esta vulnerabilidad es que el atacante remoto podría obtener acceso remoto completo a la cámara IP y al sistema Linux subyacente con permisos de root. Con acceso root al sistema operativo Linux de la cámara, un atacante podría cambiar efectivamente el código que se está ejecutando, añadir acceso de puerta trasera o invadir la privacidad del usuario accediendo a la transmisión en directo de la cámara.

- ***CVE-2022-31873:*** La cámara Trendnet IP-110wn fw_tv-ip110wn_v2(1.2.2.68) tiene una vulnerabilidad XSS a través del parámetro prefix en /admin/general.cgi.

- ***CVE-2022-31875:*** La cámara Trendnet IP-110wn fw_tv-ip110wn_v2(1.2.2.68) tiene una vulnerabilidad xss a través del parámetro proname en /admin/scheprofile.cgi

- ***CVE-2022-34138:*** Las referencias directas a objetos (IDOR) inseguras en el servidor web de Biltema IP and Baby Camera Software v124 permiten a los atacantes acceder a información sensible.

- ***CVE-2023-0773:*** La vulnerabilidad existe en la cámara IP Uniview debido a un fallo de identificación y autenticación en su interfaz de gestión basada en web. Un atacante remoto podría explotar esta vulnerabilidad enviando peticiones HTTP especialmente diseñadas al dispositivo vulnerable. La explotación exitosa de esta vulnerabilidad podría permitir al atacante obtener el control completo del dispositivo objetivo.

- ***CVE-2023-30146:*** Assmann Digitus Plug&View IP Camera HT-IP211HDP, version 2.000.022 permite a atacantes no autentificados descargar una copia de la configuración de la cámara y las credenciales del administrador.

- ***CVE-2023-30351:*** Se descubrió que la cámara IP CP3 V11.10.00.2211041355 de Shenzen Tenda Technology contiene una contraseña predeterminada codificada para root que se almacena utilizando un cifrado débil. Esta vulnerabilidad permite a los atacantes conectarse al servicio TELNET (o UART) utilizando las credenciales expuestas.

- ***CVE-2023-30352:*** Se ha descubierto que la cámara IP CP3 V11.10.00.2211041355 de Shenzen Tenda Technology contiene una contraseña predeterminada codificada para la alimentación RTSP.

- ***CVE-2023-30353:*** Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 permite la ejecución remota de código no autenticado a través de un documento XML.

- ***CVE-2023-30354:*** Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 no defiende contra el acceso físico a U-Boot a través de la UART: la contraseña Wi-Fi se muestra, y la contraseña de arranque hardcoded se puede insertar para el acceso a la consola.

- ***CVE-2023-30356:*** La falta de soporte para una comprobación de integridad en Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 permite a los atacantes actualizar el dispositivo con firmware falsificado.

- ***CVE-2023-31994***: Ciertos productos de Hanwha son vulnerables a la Denegación de Servicio (DoS). ck vector es: Cuando se envía un paquete UDP vacío al servicio de escucha, el hilo de servicio provoca un servicio no funcional (DoS) a través de WS Discovery y los servicios de descubrimiento propietarios de Hanwha. Esto afecta a la cámara IP ANE-L7012R 1.41.01 y a la cámara IP XNV-9082R 2.10.02.

- ***CVE-2023-31995:*** Hanwha IP Camera ANE-L7012R 1.41.01 es vulnerable a Cross Site Scripting (XSS).

- ***CVE-2023-31996:*** Hanwha IP Camera ANE-L7012R 1.41.01 es vulnerable a la inyección de comandos debido a la desinfección inadecuada de caracteres especiales para la función de prueba de almacenamiento NAS.

Para efectos demostrativos, se ha decidido adquirir dos cámaras IP de dos fabricantes diferentes para montar una red interna pequeña con el fin de hacer pruebas de penetración en las mismas en la búsqueda de vulnerabilidades como acceso remoto no autorizado, escucha de tráfico encubierta, interceptación de señales, entre otras especificadas en la matriz de riesgos (ver tabla 2). La red por montar es similar a la del esquema que se muestra a continuación:

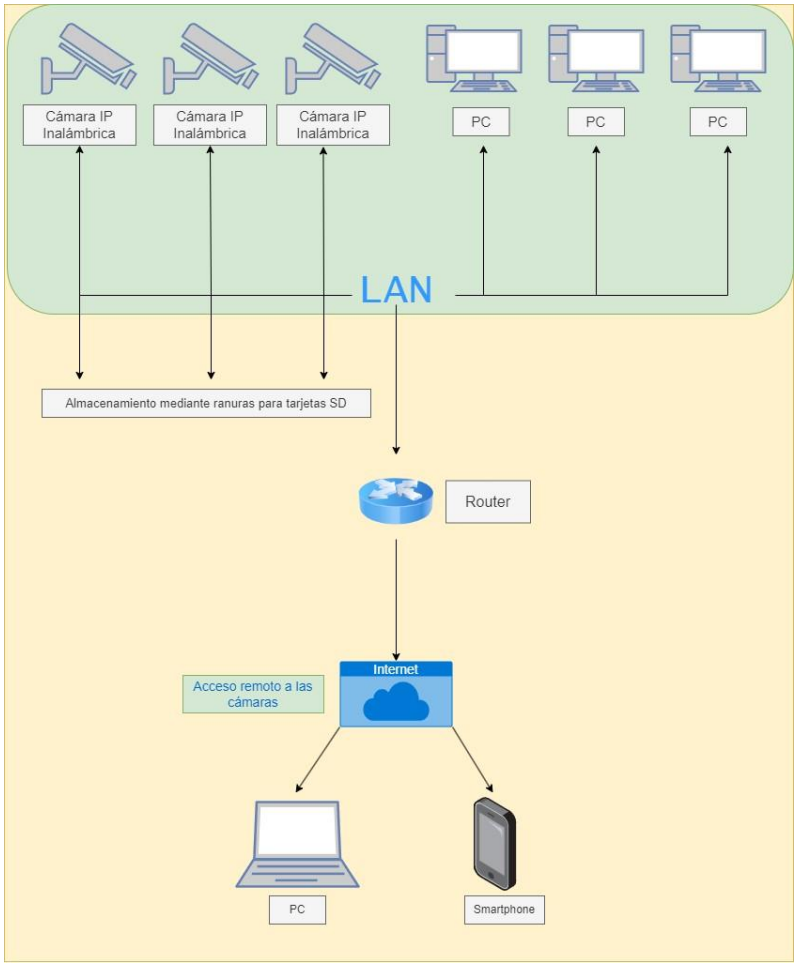

Imagen 2, diagrama de arquitectura local en una instalación de cámaras de vigilancia.

Fuente: Universidad politécnica de Valencia, España.

Cámara 1:

- Marca: YOOSE
- Resolución: 1080p
- Conectividad: 4G por WIFI 5G, por lan ethernet.
- Almacenamiento: Ranura microSD para almacenar (microSD 64gb-124gb).
- Monitoreo: Monitoreo en tiempo real en vivo por wifi mediante app.

Imagen 3: Cámara Ip Con Movimiento Infrarrojo Impermeable Wifi Full Hd

Fuente: https://articulo.mercadolibre.cl/MLC-519757958-camara-ip-con-movimiento-infrarrojo-impermeable-wifi-full-hd-_JM#position=50&search_layout=stack&type=item&tracking_id=53033ef8-2eac-4b84-a0ba-11704d8120b9

Cámara 2:

- Marca: V380
- Resolución: 720p
- Conectividad: wifi 2.4GHz.
- Almacenamiento: Ranura microSD para almacenar (hasta 32Gb).
- Monitoreo: Monitoreo en tiempo real en vivo por wifi mediante app.

Imagen 4: Cámara Ip 360°hd Onvif Camara Wifi Microsd Cctv

Fuente: https://www.falabella.com/falabella-cl/product/113960431/Camara-Ip-360%C2%B0hd-Onvif-Camara-Wifi-Microsd-Cctv/113960432

Conclusión

En conclusión, la falta de conocimiento sobre la seguridad de cámaras IP y las vulnerabilidades asociadas representa un riesgo significativo para la privacidad y la seguridad de los usuarios. La interceptación de tráfico, el espionaje no autorizado, el uso de credenciales débiles y la ausencia de cifrado en los canales de comunicación de datos son amenazas que pueden explotarse fácilmente cuando los usuarios no están informados ni toman medidas adecuadas. Para mitigar estos riesgos, es esencial que los usuarios adquieran conocimientos básicos en seguridad cibernética y apliquen buenas prácticas, como la configuración de contraseñas seguras y la implementación de cifrado en sus cámaras IP. Solo a través de una mayor concienciación y medidas proactivas, se pueden proteger eficazmente la integridad y privacidad de las cámaras de vigilancia en un entorno digital cada vez más amenazante.

Para finalizar, este manual de concientización y recomendaciones de ciberseguridad se presenta como una solución efectiva para abordar los riesgos asociados con las cámaras IP en el contexto de la domótica. Su implementación puede aumentar la conciencia de los usuarios sobre los riesgos de ciberseguridad y empoderarlos para tomar medidas efectivas de protección, lo que contribuirá significativamente a la seguridad de las viviendas y empresas en la era digital actual.

Bibliografía

- Narvaez, M. (17 de Enero de 2023). *Técnicas de recolección de datos: Qué son y cuáles existen*. QuestionPro. https://www.questionpro.com/blog/es/tecnicas-de-recoleccion-de-datos/

- Martí Martí, S. (27 de Noviembre de 2013). *Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia*. Riunet.upv.es. https://riunet.upv.es/handle/10251/34082

- Ribero-Corzo, S. M., & Prieto-Guerrero, Y. A. (2021). Identificación de riesgos en la seguridad de la información de cámaras de vigilancia domésticas en entornos IOT. https://repository.ucatolica.edu.co/entities/publication/64904c63-3163-4033-87e8-f8753b49e5c8

- *CVE - Search CVE List*. (2019). Mitre.org. https://cve.mitre.org/cve/search_cve_list.html

Anexos

N/A