TLP: WHITE

LA SEXUALIDAD EN LA ERA DIGITAL

VULNERABILIDADES EN JUGUETES SEXUALES INTELIGENTES

Autoras:
Denise Giusto
Cecilia Pastorino

CONTENIDOS

Autoras:
Denise Giusto
Cecilia Pastorino

Febrero 2021

INTRODUCCIÓN

A medida que los dispositivos de la Internet de las Cosas (IoT, del inglés Internet of Things) se cuelan en nuestro hogar ofreciendo un abanico cada vez más amplio de funcionalidades, surgen nuevas preocupaciones en cuanto a la seguridad de los datos que procesan. Aunque estos dispositivos han sido protagonistas de incontables brechas de seguridad que han derivado en la exposición de credenciales de acceso, información financiera, o datos de geolocalización, entre otros, pocos datos poseen el potencial de dañar la integridad del usuario al ser publicados como aquellos relacionados con su comportamiento sexual.

Dado que permanentemente se están lanzando al mercado nuevos modelos de juguetes inteligentes para adultos, es lógico imaginar que se están mejorando los mecanismos a la hora de procesar la información de los usuarios. Sin embargo, nuestra investigación ha dejado al descubierto que aún estamos lejos de poder vivir la sexualidad en medios digitales sin exponernos a los riesgos de sufrir un posible ciberataque. Estas fallas son más relevantes que nunca dado que se ha visto un *importante crecimiento en las ventas de juguetes sexuales* asociado a la situación sanitaria mundial y las restricciones de distanciamiento social relacionadas al COVID-19.

Aunque son varios los expertos que han dedicado su tiempo a identificar y reportar fallas de seguridad en esta industria, año tras año estos equipos han ido incorporando un rango cada vez más variado de funcionalidades: chats grupales, envío de mensajes multimedia, llamadas telefónicas, videoconferencias, sincronización con listas de canciones o audiolibros, y muchas otras más. Con cada reingeniería de código, algunas vulnerabilidades se corrigen, otras tal vez se generan y muchas otras permanecen sin cambios en las versiones actualizadas.

Entonces, ¿cuán seguros son los juguetes sexuales para adultos hoy en día? ¿Se han tomado los recaudos necesarios para proteger los datos y la privacidad de las personas? Estas son algunas de las inquietudes que abordaremos a lo largo de este whitepaper. Analizaremos el rol cada vez más importante que están teniendo estos dispositivos y las vulnerabilidades presentes en algunos de ellos, enfocándonos en la importancia de exigir (como consumidores informados) que se apliquen las mejores prácticas y estándares para garantizar la seguridad de nuestros datos y nuestra integridad.

LA EVOLUCIÓN DE LOS JUGUETES SEXUALES

Aunque muchos consumidores crean que los juguetes para adultos son una tendencia novedosa que se desprende de la inexorable fusión entre lo social y lo tecnológico en la era de la computación, la realidad es que estos dispositivos cuentan con más de un siglo de existencia. En su libro *"The Technology of Orgasm: Hysteria, the Vibrator, and Women's Sexual Satisfaction"*, Rachel P. Maines describe cómo su investigación la llevó a encontrar anuncios publicitarios de vibradores en artículos de revistas populares que datan de 1906.

En sus comienzos, inmersos en un contexto donde todo comportamiento sexual femenino que escapase al entendimiento desde una perspectiva androcentrista era considerado enfermizo, estos dispositivos eran promocionados como artefactos médicos para curar la "histeria femenina" o "enfermedad del útero", presunta afección crónica que comúnmente afectaba a las mujeres. El tratamiento de este "padecimiento" se conocía desde el 1600 y se centraba en realizar masajes genitales proporcionados por un médico o partera hasta culminar en un climax o "paroxismo histérico": el orgasmo femenino.

De este modo, según Maines, los primeros vibradores surgieron como un mecanismo capitalista para maximizar la cantidad de pacientes que era posible tratar en un día, reduciendo el tiempo promedio de cada consulta –que por entonces rondaba la hora– a unos diez minutos. Este análisis *es discutido*. Quince años después de que el primer vibrador electromecánico fuera inventado (en la década de 1880), docenas de nuevos fabricantes producían modelos alimentados tanto por cable como por una batería.

Aunque el nacimiento del vibrador esté más asociado a la opresión femenina, su aparición trajo aparejada la posibilidad de autoconocimiento para muchas mujeres en una época donde la masturbación era considerada una práctica anormal. Con la revolución causada por los movimientos feministas y el surgimiento de la industria pornográfica, nuevas formas, materiales y funcionalidades se agregaron a los antiguos vibradores, que dejaron de ser instrumentos médicos para volverse una forma de liberación sexual.

En las últimas décadas, el avance en este tipo de dispositivos se vio propulsado por los avances de la tecnología: en los 2000 hubo una nueva ola de dispositivos con capacidad de control remoto vía conexiones infrarrojas, para la década del 2010 era posible encontrar equipos controlados de forma local por aplicaciones, y ahora, en 2020, y desde hace ya algunos años, es posible encontrar dispositivos con capacidad para conectarse entre ellos a través de Internet para mantener comunicaciones larga distancia.

CARACTERÍSTICAS DE LOS JUGUETES SEXUALES INTELIGENTES

Con la aparición de la IoT, muchos fabricantes han entrado en el mercado del placer sexual integrando la capacidad de controlar los dispositivos a través de apps móviles y añadiendo interconectividad web. En la actualidad existen numerosas aplicaciones diferentes, cada una de las cuales ofrece la posibilidad de controlar una amplia gama de modelos.

Desde el punto de vista de arquitectura, la mayor parte de estos equipos poseen la capacidad de ser controlados vía Bluetooth Low Energy (BLE) desde una app instalada en un teléfono inteligente. Las principales ventajas de este protocolo es que posee requerimientos de potencia muy bajos y un aceptable rango de alcance en las comunicaciones, interoperabilidad en el mundo de los fabricantes de chipsets, y todo en un tamaño reducido. Esto hace que muchos dispositivos inteligentes del hogar, la salud, la industria automotriz e incluso los juguetes sexuales utilicen este tipo de comunicación entre el equipo y la aplicación que lo controla.

Al igual que Bluetooth, BLE opera en la banda ISM de 2.4 GHz. Sin embargo, a diferencia del Bluetooth clásico, BLE permanece en modo de suspensión constantemente, excepto cuando se inicia una conexión. Además, los tiempos de conexión propiamente dichos son de apenas unos milisegundos, a diferencia de Bluetooth, que tarda más de 100 milisegundos. En las redes Bluetooth de baja energía los dispositivos pueden ser centrales o periféricos. Los dispositivos centrales (teléfonos inteligentes, tabletas, computadoras, etc.) tienen mayor capacidad de procesamiento y son responsables de controlar los dispositivos periféricos. Los dispositivos centrales generalmente ejecutan software creado específicamente para interactuar con dispositivos periféricos. Estos últimos actúan como sensores, que recogen datos y los envían a los dispositivos centrales para ser procesados. Esta es la clave del bajo consumo de los periféricos BLE: no procesan los datos, sólo los recogen y los transmiten.

Por último, la aplicación se encarga de configurar las opciones del dispositivo y de controlar el proceso de autenticación del usuario. Para ello, suele conectarse a un servidor en la nube, que almacena la información de la cuenta de la persona. En algunos casos, la aplicación también actúa como intermediaria entre varios usuarios que desean utilizar funciones como el chat, la videoconferencia o la transferencia de archivos, o si los propietarios de los dispositivos quieren ceder el control de estos a usuarios remotos.

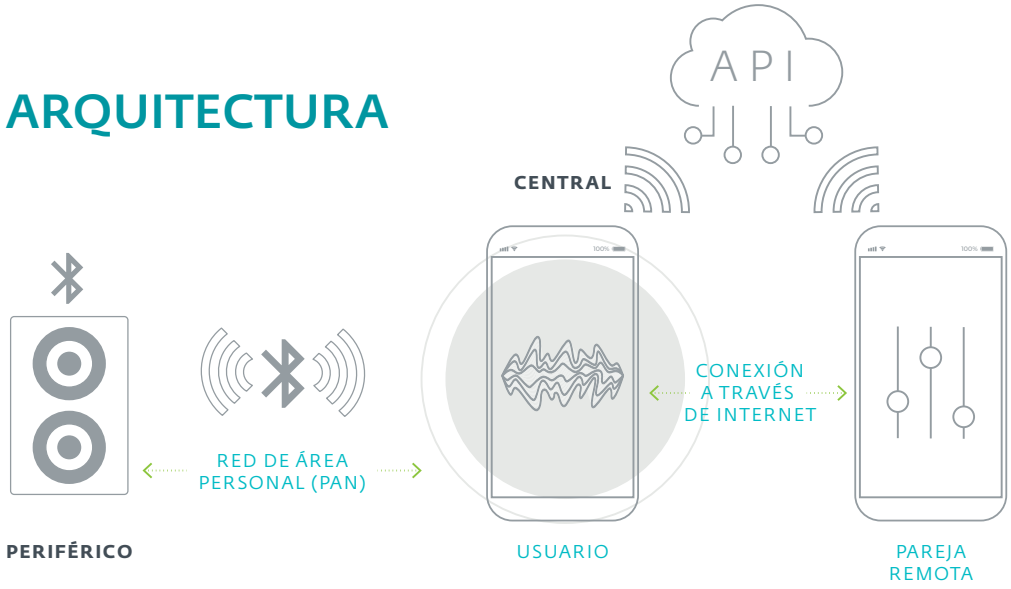

Imagen 1 // Arquitectura de un juguete sexual inteligente.

Esta arquitectura presenta varios vectores de ataque que podrían utilizarse para comprometer la seguridad de los datos que se procesan: Interceptar la comunicación local entre la app de control y el dispositivo, entre la app y la nube, entre el teléfono remoto y la nube, o atacar directamente el servicio online del fabricante (API). Por supuesto, no todos los ataques tienen lugar a través de las conexiones de red, y algunos escenarios maliciosos podrían ser lanzados usando malware previamente instalado en el teléfono o explotando fallos en el sistema operativo del teléfono. Sin embargo, en este artículo sólo abordaremos las vulnerabilidades presentes en la propia aplicación y el dispositivo.

A pesar de que ya han sido sometidos al escrutinio de muchos investigadores de seguridad ([1], [2], [3], [4], entre otros), nuestra investigación demostró que estos dispositivos continúan manteniendo fallas de seguridad que podrían poner en jaque la seguridad de los datos almacenados, así como la privacidad e incluso la integridad del usuario. Estas vulnerabilidades van desde procedimientos de autenticación deficientes hasta dispositivos que constantemente anuncian su presencia, permitiendo que cualquiera se conecte a ellos.

¿POR QUÉ ES TAN CRÍTICA LA SEGURIDAD EN JUGUETES SEXUALES?

No es una novedad que muchos dispositivos de la IoT presentan vulnerabilidades. En publicaciones anteriores ESET ha analizado importantes fallos descubiertos en múltiples centrales inteligentes de uso hogareño, así como en *cámaras initeligentes*. Recientemente, los *investigadores de ESET descubrieron KrØØk*, una vulnerabilidad crítica que afectaba el cifrado de más de mil millones de dispositivos Wi-Fi. Sin embargo, en el caso de los juguetes sexuales, la sensibilidad de la información que procesan estos dispositivos resulta extremadamente crítica: nombres, preferencias y orientaciones sexuales, lista de parejas sexuales, datos de utilización del equipo, fotos y vídeos íntimos. Todas estas piezas de información pueden llevar a consecuencias desastrosas en caso de caer en las manos incorrectas.

¿Quiénes pueden interesarse en este tipo de información? En lugares como *Alabama* en Estados Unidos, la venta de dispositivos sexuales es ilegal, aunque aún pueden encontrarse algunos modelos promocionados bajo eufemismos médicos, tal como ocurría en el año 1906 de acuerdo a los hallazgos de Maines en su investigación. Por otra parte, muchos países profundamente conservadores cuentan con leyes estrictas que prohíben algunas o todas las formas de actividad sexual homosexual, prematrimonial

o extramatrimonial. En estos países, *mayormente de África y Asia*, la publicación de información íntima sobre el comportamiento sexual de un individuo y de sus parejas puede derivar en arresto y posteriormente la cárcel o, incluso, la pena de muerte.

En este contexto, ¿qué ocurriría si las autoridades de un país o región emprendieran una campaña de opresión basada en la expropiación forzosa de datos sobre las empresas que los procesan o la explotación de fallos o debilidades en dispositivos sexuales como forma de identificar, geolocalizar y perseguir a homosexuales, infieles, o cualquier otra minoría o grupo social según sus elecciones sexuales?

Sumado a las preocupaciones de espionaje gubernamental, los juguetes sexuales inteligentes tampoco están exentos de la posibilidad de ser comprometidos por ciberatacantes. Nuevas formas de sextorsión aparecen en el radar si consideramos el material íntimo al que tienen acceso las aplicaciones que controlan estos equipos.

Algunos antecedentes ya existen y nos ayudan a tomar dimensión de la escala que podrían tener las posibles consecuencias. El *ataque al "sitio de citas" Ashley Madison* es quizás el primer ejemplo que se nos viene a la cabeza. Luego de que se publicaran los nombres de más de 30 millones de usuarios de la plataforma para "adúlteros", un sinnúmero de *reportes* de divorcios y suicidios alcanzaron los medios de comunicación.

Sumado a la preocupación por la confidencialidad de los datos, debemos considerar la posibilidad de que vulnerabilidades en aplicaciones para controlar juguetes sexuales permitan la instalación de malware en el teléfono o la modificación del firmware de los juguetes. Estas situaciones podrían derivar en ataques de DoS (Denegación de Servicio) que bloqueen el envío de cualquier comando, o que un dispositivo sea convertido en un instrumento capaz de realizar acciones maliciosas y propagar malware o, incluso, que sea deliberadamente modificado para causar daños físicos al usuario; por ejemplo, recalentándose y explotando.

Paralelamente, no podemos hablar sobre las implicancias de un ataque a un dispositivo sexual sin replantearnos la significancia del abuso sexual en el marco de la transformación digital por la que atraviesa la sociedad. ¿Cuáles son las consecuencias de que alguien pueda, sin consentimiento, tomar control de un dispositivo sexual mientras está siendo utilizado para enviarle órdenes diferentes? ¿La legislación vigente contempla la posibilidad de penar este comportamiento? ¿Podríamos describir esto como un acto de abuso sexual?

La noción de cibercrimen adopta un nuevo semblante si lo miramos desde la perspectiva de la invasión a la privacidad, el abuso de poder, y la falta de consentimiento ante un acto sexual —algunos de estos dispositivos son wearables y una vulnerabilidad podría permitir que cualquiera dentro de cierto rango pueda comenzar a utilizarlos. Aunque la mayor de los países cuenta hoy en día con un marco legal que tipifica varios tipos de ciberdelito, aún no hemos llegado al punto de evaluar las nuevas formas de abuso que se desprenden de sistemas digitales que poco a poco se han ido incorporando a la intimidad de una gran cantidad de usuarios.

Solo una cosa está clara: el consentimiento obtenido de forma fraudulenta no es consentimiento, y este vacío legal en las actuales leyes deberá ser resuelto en un futuro cercano para garantizar la integridad sexual, física y psicológica de los usuarios en torno al espacio digital.

NUESTRA INVESTIGACIÓN

El objetivo de nuestra investigación fue determinar el nivel de seguridad en aplicaciones para Android destinadas a controlar los modelos más completos de las principales marcas en el rubro del placer sexual, para determinar en qué medida se garantiza la confidencialidad de los datos de los usuarios.

Una de las dificultades que surge a la hora de analizar dispositivos sexuales —y equipos IoT en general— es la gran variedad de modelos disponibles en el mercado, cada uno con su propio firmware y aplicación

para controlarlos. Por tal motivo, decidimos limitar nuestro análisis a dos de los fabricantes más conocidos del mercado internacional, obteniendo uno de cada uno de los siguientes productos: el Max de Lovense y el Jive de We-Vibe.

En primer lugar, descargamos las aplicaciones de los fabricantes disponibles en Google Play Store para controlar estos juguetes sexuales (*We-Connect* y *Lovense Remote*), y usamos herramientas de análisis automático de vulnerabilidades y técnicas de análisis manual para identificar fallas en sus implementaciones.

Device	App Name	App packet	Version	Hash
Jive	We-Connect	com.standardinnovation.weconnect	3.0.3	FC7780F593263975E11391000229EC51C831CEEC
			4.3.1	0E9F9E72E8BC0C392A285C6F5FDF33D21267DFC1
			4.4.1	E35006AA28B4539758BD72FCD8715E7516906F75
Max	Lovense Remote	com.lovense.wear	3.4.6	B7A8735C9F16252E564F841ECC9861C43F0B1D68
			3.5.8	A0CBBC09997038D8658B4E3BD644B7357A32123E
			3.7.1	E167CA3972ADB00D7B0141CFD7D2B8687139AD0E
			3.8.1	852E87FCBF774117342407A3E5D48C7AB7F38EBE
			3.8.4	8280097D01DFFC2AC75B1EC945CB77E868EC0DB9
			3.8.6	954D7562C75D71CDE30A73BEA5A0884C510CE0A1

Tabla 1 // Detalles de las aplicaciones analizadas.

En las secciones siguientes se detallan algunos de los problemas de seguridad que descubrimos en cada aplicación y dispositivo durante nuestra investigación. Ambos desarrolladores recibieron un informe detallado de las vulnerabilidades y sugerencias acerca de cómo corregirlas.

Al momento de la publicación de este artículo, todas las vulnerabilidades han sido solucionadas.

We-Vibe

Una de las marcas más conocidas en el mercado de los juguetes sexuales es We-Vibe. Bajo esta marca se vende una amplia gama de productos, incluidos algunos dispositivos inteligentes. Un aspecto interesante es que muchos de ellos están diseñados para poder ser utilizados como wearables, pudiendo llevarse puestos a lo largo del día. Este último factor fue la razón por la cual elegimos comprar el modelo Jive para realizar esta investigación, presuponiendo que al ser wearables son propensos a ser utilizados en entornos inherentemente inseguros.

Imagen 2// El modelo Jive de We-Vibe

Cuando comenzamos nuestra investigación preliminar nos encontramos con que ya se había publicado información que hablaba de las principales vulnerabilidades descubiertas en el dispositivo. Por ejemplo, en 2016 especialistas presentaron en Defcon una charla titulada *"Breaking the Internet of Vibrating Things"* en la cual detallaron graves fallos de seguridad descubiertos en la aplicación We-Connect, la cual se utiliza para todos los modelos inteligentes del fabricante. En concreto, la recopilación de información sensible sin la autorización del usuario provocó una serie de demandas contra Standard Innovation (ahora parte de WOW Tech Group) y el consecuente *pago de casi 3.7 millones de dólares a los damnificados* en 2017.

Tras el pago de la multa, la compañía decidió realizar cambios en la app para eliminar cualquier rastro de información personal de sus sistemas. Actualmente, la aplicación no almacena datos personales de los usuarios, aunque su política de privacidad sí estipula que se utilizará un token en conjunto con la IP del dispositivo para para identificar al equipo. Por otra parte, recolecta datos como el idioma, modelo de teléfono, versión del sistema operativo, fecha y hora, e identificadores únicos de equipo, y se ofrece al usuario la opción de compartir información adicional sobre el uso del dispositivo activando esta función en los ajustes de la aplicación.

Otra de las mejoras introducidas en la aplicación en los últimos años ha sido la inclusión de *certificate pinning* (comprobación de certificados), lo que significa que la aplicación comprueba que el servidor al que se conecta es legítimo. Utilizando esta técnica de validación en el lado del cliente, la aplicación compara el certificado del servidor con una lista de certificados de confianza integrada en la propia aplicación. Si no coinciden, la conexión se interrumpe. Aunque esto aumenta la seguridad para los usuarios finales, no incluyeron ningún tipo de mecanismo de chequeo de integridad del ejecutable, con lo cual es sencillo evadir las técnicas de *certificate pinning* con propósitos de estudio, modificando el código del APK para incluir un certificado autofirmado o inyectando la aplicación con herramientas de ingeniería inversa como *Frida*.

Conexión Bluetooth

Al igual que muchos dispositivos IoT, el Jive utiliza Bluetooth Low Energy para conectarse y comunicarse con el dispositivo móvil del usuario. Las principales características de seguridad que incorpora BLE son el cifrado de 128 bits y la autenticación. La comunicación a través de BLE es segura en dispositivos que ya han verificado una conexión. Sin embargo, para conectarse, los dispositivos deben emparejarse primero, y aquí es donde reside la principal vulnerabilidad de los sistemas BLE. Para conocer de forma detallada cómo funciona este protocolo puedes visitar *nuestro artículo en WeLiveSecurity*.

Durante la primera etapa de emparejamiento, el Jive y el dispositivo móvil intercambian información básica sobre sus capacidades para descubrir cómo proceder con la conexión. Es decir, se identifican en la red, explican qué son (equipo, marca, modelo, etc.) y qué pueden hacer. Este intercambio no está cifrado.

La segunda fase de emparejamiento está dedicada a generar e intercambiar claves. Es en este punto que las conexiones BLE pueden ser manipuladas: si la conexión no está asegurada adecuadamente, los atacantes pueden tomar el control de los dispositivos y los datos que transmiten.

Por último, la vinculación es el proceso durante el cual los dispositivos almacenan los datos de autenticación que intercambiaron durante el primer emparejamiento, lo que les permite recordarse mutuamente como seguros cuando se vuelven a conectar en el futuro.

Existen métodos para asegurar la segunda fase, como el uso de claves temporales para autorizar la conexión o el uso de BLE Secure, que se introduce en la versión 4.2 e implementa el algoritmo Diffie-Hellman para la generación de claves, además de introducir un proceso más complejo de autenticación. Sin embargo, el Jive no implementa estos métodos, lo que lo hace particularmente vulnerable a ataques de hombre en el medio (Man-in-the-middle).

Por otro lado, dado que el Jive necesita estar anunciando permanentemente su conexión para que el usuario pueda conectarse a él, cualquier persona podría utilizar un simple escáner de Bluetooth para encontrar dispositivos cercanos. De hecho, esto fue lo que hizo el investigador Alex Lomas, quien *caminó por las calles de Berlin con su smartphone descubriendo juguetes sexuales* anunciando su presencia mediante avisos de conexión Bluetooth. Lo anterior demuestra que incluso en entornos hogareños se presenta la posibilidad de una intrusión inesperada al dispositivo.

Imagen 3// Descubrimiento de juguetes sexuales disponibles en las inmediaciones mediante un escáner Bluetooth.

En el caso de nuestro equipo Jive, estos riesgos se ven potenciados ya que es un *wearable* diseñado para que el usuario lo lleve "puesto" a lo largo del día –en restaurantes, fiestas, hoteles o cualquier otro ambiente público. En estas situaciones, un atacante podría identificar el dispositivo y utilizar la fuerza de la señal del dispositivo como una brújula para ir acercándose hasta encontrar a la persona exacta que lo lleva puesto.

En la Imagen 3 vemos una captura de pantalla de un escáner Bluetooth en la que se encuentran tanto el Jive como el Max de Lovense (de nombre "LVS-B018", dispositivo que analizaremos en la siguiente sección). Allí vemos que el Jive se anuncia con el nombre del modelo, haciendo sencilla su identificación. En la otra imagen se observa la potencia de la señal en -69 dBm. A medida que el escáner se acerca al dispositivo la potencia de la señal aumenta, permitiendo identificar su ubicación exacta.

Si bien mientras el Jive está conectado al móvil del usuario dejará de anunciar su conexión, al cerrar la aplicación en el equipo la conexión se corta y el juguete empieza a anunciarse nuevamente. Teniendo esto en cuenta, existen antenas "jammer" que se pueden utilizar para bloquear las señales Bluetooth, las cuales también podrían ser utilizadas por un atacante para desconectar el dispositivo periférico y posteriormente tomar control de este. De cualquiera de estas formas el Jive puede ser conectado a un equipo malicioso en las inmediaciones cuando el dispositivo legítimo del usuario no esté conectado a el.

Una vez que se encuentra un Jive disponible, un atacante ni siquiera necesita instalar la aplicación oficial del fabricante, ya que la función de Bluetooth web incluida en la mayoría de los navegadores actuales le permite conectarse e interactuar con el Jive (y otros modelos) a través de los sitios web existentes que facilitan la interacción con este tipo de juguetes sexuales. La grave preocupación por la privacidad fue lo que llevó a *Apple a rechazar la implementación de esta API Web Bluetooth en Safari*.

BLE MitM

Un ataque de Man-In-The-Middle involucra un dispositivo malicioso que pretende ser central y periférico al mismo tiempo y engaña a otros dispositivos de la red para que se conecten a él. En este caso, el atacante no sólo puede escuchar el tráfico de los dispositivos conectados a una distancia de entre 6 y 8 metros, sino que también puede enviar paquetes maliciosos para controlar el equipo o explotar vulnerabilidades. Este tipo de ataques solo puede evitarse con un método de emparejamiento apropiado y seguro.

En el Jive, el dispositivo se empareja mediante el método "Just Works", que es el menos seguro de todos (y, lamentablemente, el que viene de forma predeterminada en la mayoría de los equipos IoT). En ese método la clave temporal que los dispositivos intercambian durante la segunda fase de emparejamiento se establece en 0, y los dispositivos generan el valor de la clave a corto plazo en función de eso. Este método es altamente vulnerable a ataques de MiTM, ya que cualquier dispositivo puede conectarse con la clave temporal 0. Es decir que, en términos prácticos, el Jive se vinculará automáticamente con cualquier teléfono móvil, tableta o computadora que se lo solicite, sin realizar ningún tipo de verificación o autenticación.

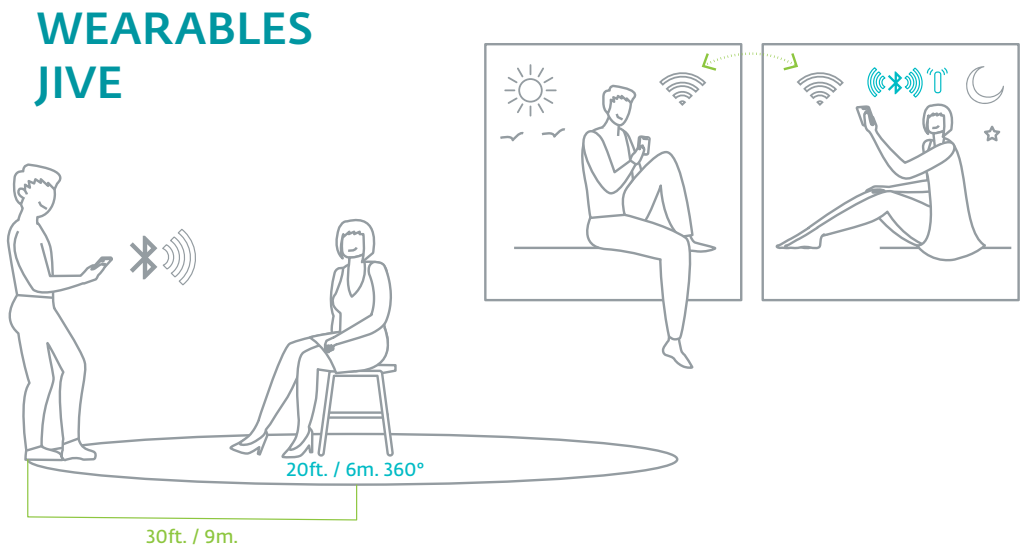

Imagen 4// El Jive de We-Vibe es un equipo wearable, diseñado para llevarse puesto.

Este no es el único problema: mientras el Jive no esté vinculado a la app, estará constantemente anunciando su presencia y esperando una conexión. Esto hace que un atacante pueda fácilmente tomar el control del dispositivo estando a menos de 9 metros de él.

En nuestra prueba de concepto utilizamos el framework *BtleJuice* y dos antenas (denominadas *dongles*, en inglés) de Bluetooth LE para replicar un ataque de Man-in-the-Middle entre un usuario y el Jive. Pueden acceder a la demostración en el siguiente video:*https://youtu.be/1o-qEOau1hg*

En ella, simulamos un escenario donde un atacante primeramente toma el control del Jive (al cual se conecta directamente debido a su falta de autenticación) y luego anuncia un "dummy", es decir, un falso dispositivo Jive, que configura basándose en la información que anunció el Jive original. Luego, cuando el usuario desea vincularse con el juguete, en realidad lo hará con el falso dispositivo creado por el atacante.

De esta forma, el atacante logra capturar todos los paquetes enviados por el usuario al juguete mediante la interfaz web de BtleJuice y así obtener información sobre los modos de uso, intensidad de vibración, etc. También tiene la posibilidad de editar los comandos interceptados, modificando el modo de vibración o la intensidad. Por último, puede generar sus propios comandos y enviárselos al juguete por más que el usuario no esté interactuando con él.

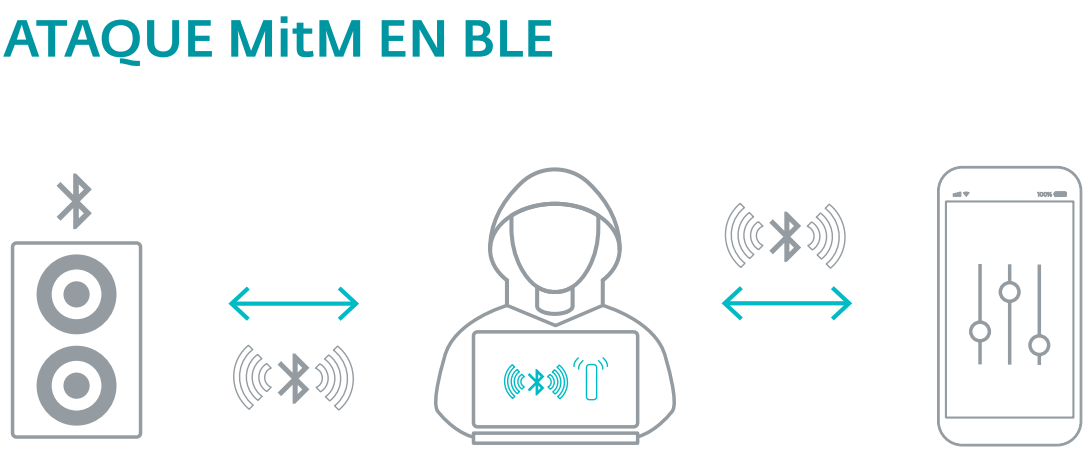

Imagen 5// Arquitectura de un ataque MitM entre un equipo Bluetooth y la app que lo controla.

Metadatos

Al analizar qué ocurría con los archivos multimedia que se compartían entre los usuarios de We-Connect durante las sesiones de chat, descubrimos que estos se guardan dentro de las carpetas de almacenamiento privado de la aplicación –es decir, no pueden ser accedidos por otras aplicaciones instaladas en el equipo– y que se eliminan inmediatamente cuando termina el chat, lo cual, desde el punto de vista de la privacidad, es algo positivo. Sin embargo, cuando investigamos qué pasaba con los metadatos de los archivos, nos sorprendió descubrir que seguían estando en el archivo compartido. Esto significa que cada vez que los usuarios envían una foto a un teléfono remoto, también pueden estar enviando información sobre sus dispositivos y su geolocalización exacta.

Almacenar información sensible sin protección en el dispositivo nunca es una buena idea desde el punto de vista del desarrollo, incluso cuando se utilizan las carpetas privadas de las aplicaciones para este fin. En este escenario, un usuario malintencionado con un teléfono rooteado podría acceder a estos archivos, analizarlos utilizando un sitio web como *metapicz*, y obtener información sobre los usuarios que compartieron originalmente las imágenes, incluyendo la ubicación GPS y el modelo de smartphone.

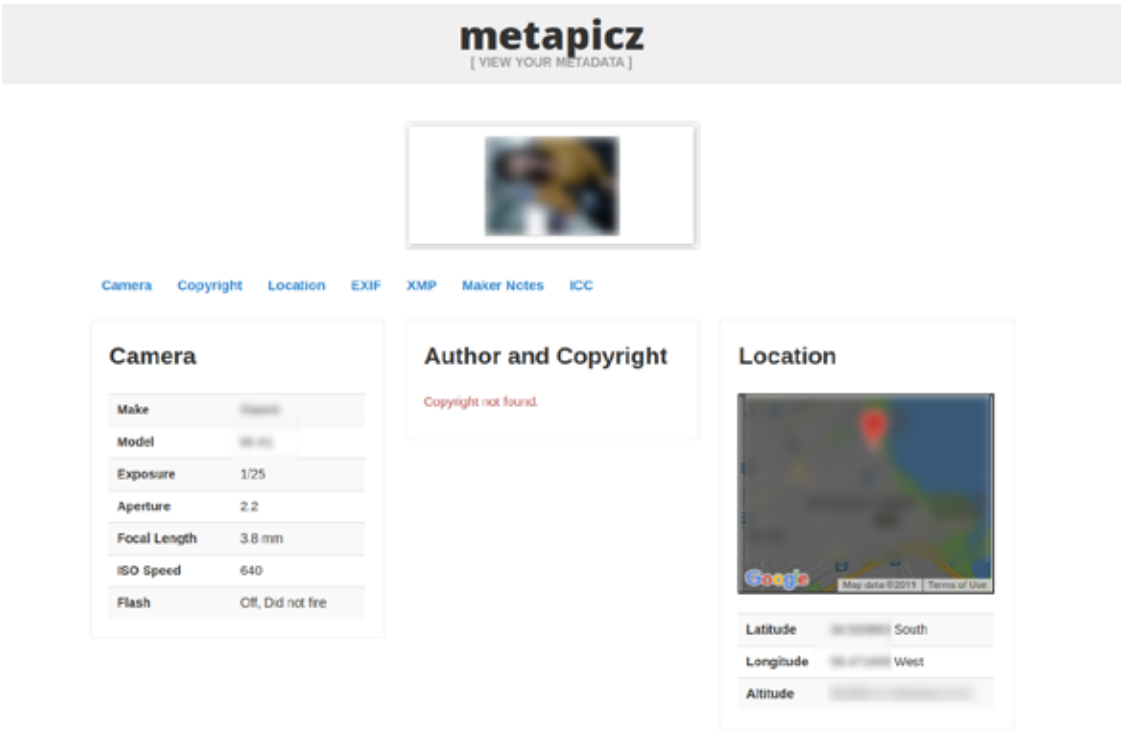

Imagen 6// Metadatos en las imágenes enviadas por el chat de la app de We-Vibe.

Esto es sumamente relevante porque muchos usuarios ceden intencionadamente el control de su dispositivo a completos desconocidos al compartir públicamente su URL de acceso en línea. Al hacerlo, pueden estar compartiendo inadvertidamente más información de la que creen.

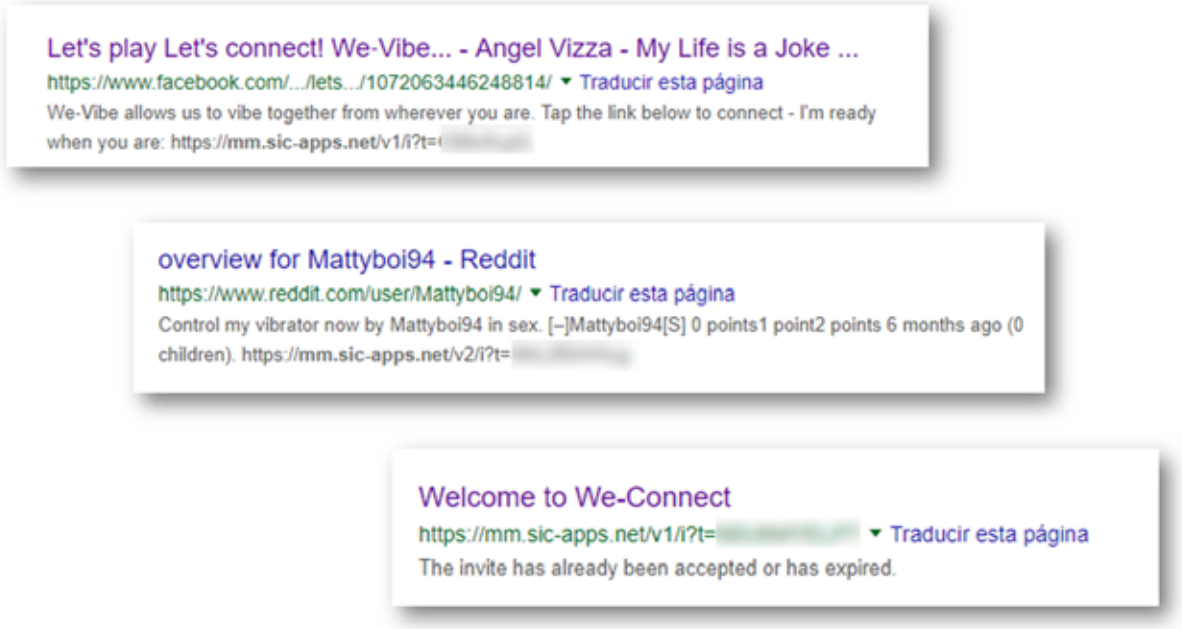

Imagen 7// Usuarios que comparten sus tokens de forma pública.

PIN de bloqueo

La app ofrece a sus usuarios la posibilidad de configurar un PIN de cuatro dígitos para poder acceder a ella, pero no posee sin ningún tipo de penalidad por intentos errados, con lo cual no se tarda mucho en lograr saltar el control mediante fuerza bruta con un *bad USB*. Como el número de posibilidades es relativamente bajo, un atacante podría probar todas las combinaciones posibles y conseguir el PIN en menos de 12 horas. Puedes ver una demostración de esto en el siguiente vídeo:

https://www.youtube.com/watch?v=8eYSUoyS9jw

Una solución a este problema podría ser aumentar la complejidad de la contraseña, añadir intervalos de retardo fijos o exponencialmente crecientes para la reintroducción del PIN después de un cierto número de intentos incorrectos, y/o modificar la interfaz gráfica de usuario para incluir una cuadrícula de botones en lugar de una entrada de teclado.

Lovense

El segundo de los dispositivos que se analizaron fue el masturbador Max de Lovense. Lo interesante de este dispositivo es su capacidad de sincronizarse con su contraparte remota, que puede ser alguno de varios modelos de Lovense. La sincronización permite que el equipo replique los movimientos de su par remoto. Este escenario resulta interesante desde un punto de vista de hacking ya que un atacante podría tomar control de ambos dispositivos comprometiendo solamente uno de ellos.

Imagen 8// El Max de Lovense

En comparación con el Jive, una buena noticia es que las fotos no poseen metadatos al momento de ser receptadas por el equipo remoto. Esta aplicación también ofrece la posibilidad de configurar un patrón de desbloqueo de cuatro dígitos, pero en este caso la interfaz se presenta como una grilla de botones, dificultando el proceso de fuerza bruta.

Preocupaciones de privacidad

Diseño inseguro

Lo primero que capta la atención en lo que respecta a la aplicación de Lovense son algunas polémicas decisiones de diseño que podrían poner en riesgo la confidencialidad de imágenes íntimas enviadas por los usuarios. La más significativa de estas características es la opción de reenvío de imágenes, que permite al receptor compartir material con terceros sin solicitar consentimiento, o sin siquiera emitir una notificación, al creador del contenido.

La app también brinda la posibilidad de descargar el contenido multimedia que se ha recibido, nuevamente sin notificar a quien compartió el material en primer lugar. Esta funcionalidad permite que las imágenes recibidas por el teléfono remoto se almacenen en el sistema de archivos compartidos, pudiendo ser accedidas por otros aplicativos instalados en el teléfono (incluyendo malware). Por ejemplo, podrían aparecer listadas dentro de Google Fotos, siendo incluso respaldadas en la nube mediante estos servicios de terceros.

Aunque el chat incluye la funcionalidad de borrado de mensajes, esta opción solamente sirve para ocultar el mensaje del chat local y no elimina el contenido del teléfono remoto. Esto podría generar malentendidos, haciendo pensar al usuario que sus imágenes previamente compartidas se han eliminado del teléfono receptor y se encuentran seguras, cuando en verdad no es así.

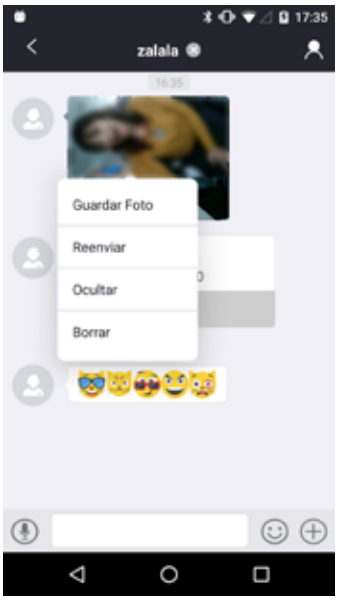

Imagen 9// Menú de opciones sobre archivos multimedia en Lovense Remote.

De hecho, incluso si elimina o bloquea a un usuario, esa persona seguirá teniendo acceso al historial de chat y a todos los archivos multimedia compartidos. En las últimas versiones de la aplicación, hay una opción extra que borra el contenido del teléfono remoto, pero esa opción solo está disponible durante dos minutos después de enviar una imagen y luego desaparece por completo. Además, la función de captura de pantalla permanece habilitada, lo que permite a un usuario malintencionado tomar capturas de pantalla de cualquier cosa en el chat.

Las imágenes enviadas al dispositivo remoto dependen únicamente de HTTPS para su protección, no hay cifrado de extremo a extremo y, cuando se almacenan en el servidor, su secreto depende del secreto de sus nombres de archivo, que son identificaciones aleatorias generadas por el servidor al momento de subida. Estas imágenes permanecen en el servidor durante al menos siete días -según se detalla en la política de privacidad-, aunque la mayoría de ellas permanecen allí mucho más tiempo. En última instancia, una vez que los usuarios han compartido un contenido, pierden todo el control de este.

A pesar de que estas no son vulnerabilidades per se, estos hallazgos constituyen serios problemas de privacidad. Hoy en día, la mayoría de las aplicaciones de mensajería instantánea permiten a los usuarios eliminar mensajes en cualquier momento que lo deseen o configurar temporizadores para su borrado automático. Notifican si el contenido que está recibiendo se ha reenviado y aplican cifrado de extremo a extremo. Si se está utilizando un chat secreto en Telegram, no es posible tomar capturas de pantalla. A medida que las aplicaciones de mensajería instantánea cotidianas se vuelven más seguras, uno esperaría lo mismo de aplicaciones diseñadas específicamente para compartir contenido sexual.

Divulgación no intencional de información

A pesar de que los usuarios se muestran públicamente a otros con un nombre de fantasía, la app Lovense Remote utiliza la dirección de correo electrónico que se haya registrado al momento del primer inicio de sesión como identificador de cada usuario en los procesos de envío de mensajes. Más aún, la dirección de correo electrónico se comparte entre todos los teléfonos involucrados en cada chat, y se almacena en texto plano en diferentes archivos locales, como en el archivo de preferencias compartidas wear_share_data.xml.

De esta forma, un usuario malicioso podría acceder al listado de las direcciones de correo de los usuarios que ha añadido como contactos. Con esta información, el atacante podría iniciar un proceso de identificación y reconocimiento de usuarios sin su consentimiento mediante la recolección de información en línea, sirviendo como pie para posteriores ataques de Ingeniería Social y pudiendo derivar en sextorsión.

Imagen 10// Preferencias compartidas de la app de Lovense para sexting donde se publica información sensible de otros usuarios.

También es posible realizar el proceso inverso y encontrar la cuenta de usuario asociada a un determinado correo electrónico, dado el caso de que dicha dirección de correo esté registrada en el servidor. Esto es posible simplemente realizando una petición GET al servidor, indicando el correo electrónico cuya existencia se desea constatar.

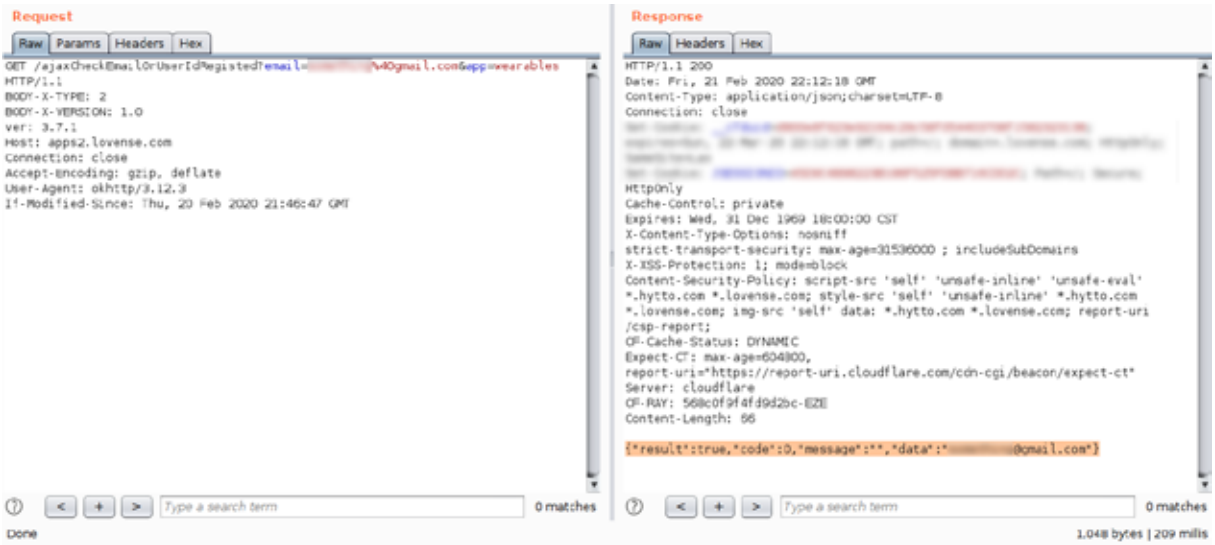

Imagen 11// Esta petición GET consulta si una determinada cuenta de correo concuerda con un usuario en la plataforma de Lovense. En este caso, el resultado es positivo.

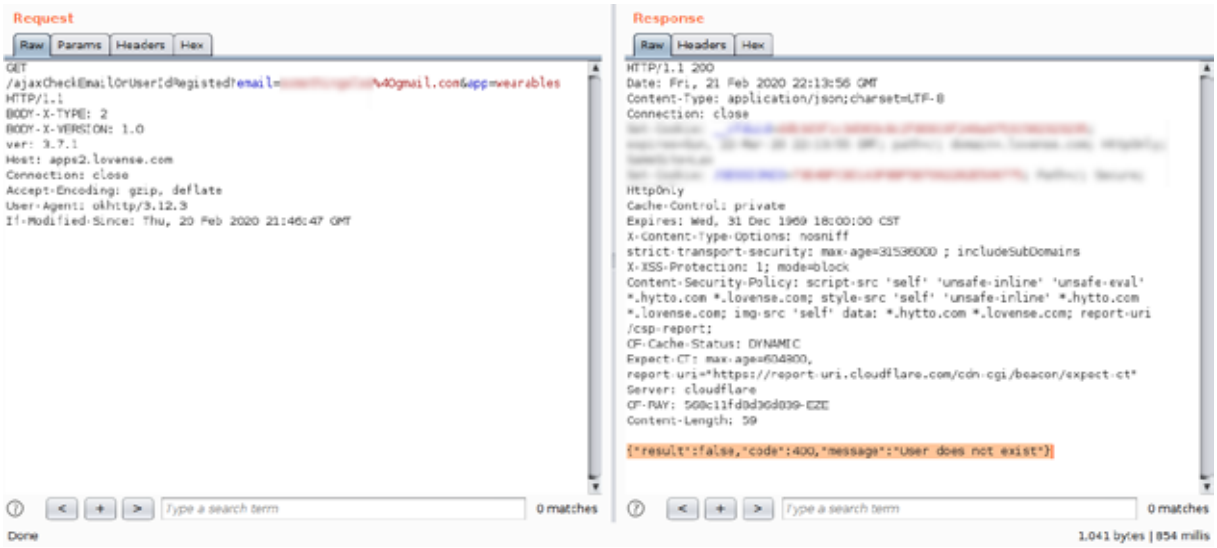

Imagen 12// En contraposición a la imagen 11, el servidor responde de manera negativa a una consulta sobre una dirección de correos.

Control remoto vía fuerza bruta de tokens

Dentro de las opciones de control remoto que ofrece la aplicación, además de poder ceder el control del equipo con un usuario agregado a la lista de contactos, es posible generar una URL de formato `https ://api2.lovense.com/c/<TOKEN>`, donde `<TOKEN>` es un conjunto de 4 caracteres alfanuméricos. De esta manera, el usuario remoto puede controlar el equipo simplemente ingresando a la URL desde su navegador.

Algunos usuarios deciden compartir sus tokens de forma pública, ya sea que lo realicen en un entorno privado, o bien, como parte de un servicio de *modelo de cámara web*. Comunidades en Reddit son la opción preferida el momento de compartir tokens de manera anónima. La utilización del correo electrónico como ID del usuario en los archivos de configuración podría hacer peligrar la privacidad e integridad física de personas que ni siquiera sospechan cuánta información están verdaderamente exponiendo.

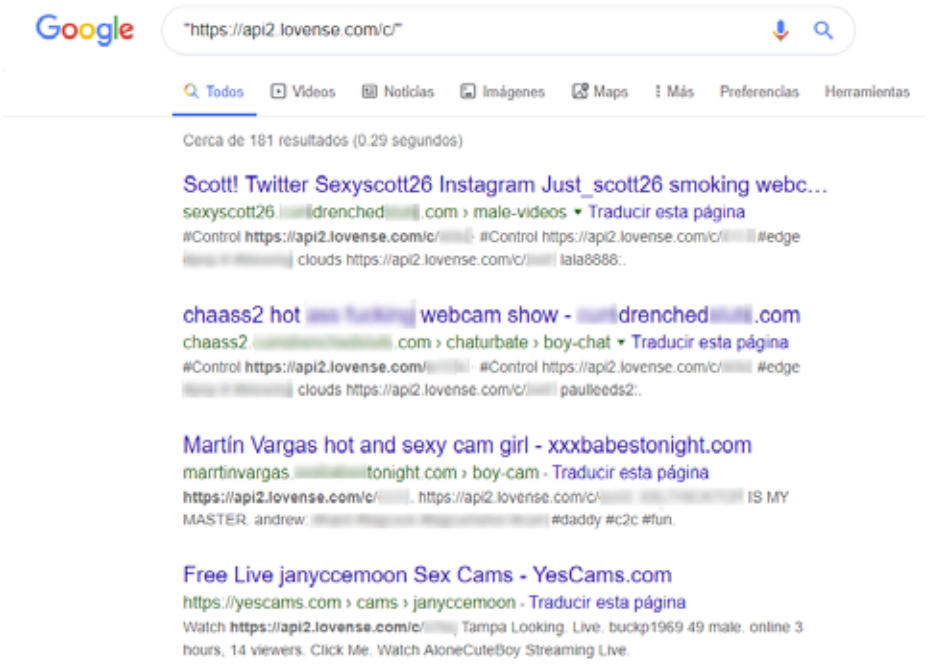

Imagen 13// Tokens de control remoto de dispositivos Lovense que pueden encontrarse rápidamente en motores de búsqueda o redes sociales.

Aunque la app advierte a sus usuarios que el token se desactiva automáticamente luego de 30 minutos de inactividad o cuando el usuario genera un nuevo código desde la aplicación, hemos podido comprobar que algunos tokens permanecían activos mucho tiempo después de concluida la media hora. No pudimos determinar un período de tiempo específico antes del vencimiento ni las causas de la expiración, pero algunos tokens permanecen activos durante días.

Sorprende que, tratándose de un token tan corto con pocas posibilidades de combinaciones (1.679.616 posibles tokens para una app con más de un millón de descargas), el servidor no posee ningún tipo de protección contra fuerza bruta. Cabe la pregunta entonces, ¿es posible encontrar por fuerza bruta tokens válidos (que hayan existido alguna vez) y activos (que aún no hayan expirado y todavía permitan el control remoto)?

Para comprender cómo funcionan los tokens, usamos la aplicación Lovense Remote, algunos teléfonos inteligentes de prueba, el dispositivo Max de Lovense y un navegador web. Creamos tokens en un entorno controlado y estudiamos el tráfico de la red mientras accedíamos a ellos a través del navegador y otros teléfonos.

Cuando se peticiona por un token inexistente, el servidor redirecciona a `/redirect` y devuelve el mensaje JSON `{“result”:true,”code”:404,”message”:”Page Not Found”}`. Por el contrario, si el token es válido, el servidor redirecciona a otra URL cuyo formato es `https://[apps|api2].lovense.com/app/ws/play/<SID>`, que a su vez redirecciona a `https://[apps|api2].lovense.com/app/ws2/play/<SID>`. El `<SID>` es el ID de sesión: una cadena de texto similar a un MD5 creada al momento de generar el token que identifica unívocamente al usuario y al ID del dispositivo para el cual fue creado. Un token expira cuando se vence su tiempo límite (presumiblemente) o cuando alguien ya ha ingresado a la última URL tras concretar todo el proceso de redirecciones.

De lo anterior puede deducirse que es posible discriminar entre tokens válidos, activos o expirados según la respuesta del servidor. Para comprobar lo anterior, primero enumeramos docenas de tokens: creamos algunos de ellos con nuestro dispositivo y luego agregamos otros tokens aleatorios. La mayoría de los tokens generados por nuestro dispositivo ya habían expirado, pero uno aún estaba activo. Luego programamos un script Python simple y lo usamos contra este conjunto de tokens. Cuando este script encuentra un token válido, abre la URL final en el navegador y verifica si la sesión ha expirado con la ayuda de una extensión de Chrome que diseñamos para el propósito de esta investigación. Si se encuentra que la sesión está activa, envía un mensaje a través de un bot de Telegram a la cuenta especificada, notificándole del nuevo panel de control encontrado. Grabamos un video de prueba de concepto, disponible aquí:

https://youtu.be/5lWSaJC3WWU

Trabajando junto con el fabricante, pudimos confirmar que era posible encontrar tokens de usuarios aleatorios utilizando la fuerza bruta. Esta vulnerabilidad es extremadamente grave, ya que permite que un atacante pueda fácilmente secuestrar remotamente equipos que estén a la espera de conexiones mediante tokens activos sin el consentimiento o conocimiento del usuario. La remediación de este fallo podría incluir aumentar el alfabeto y la longitud del token para reducir la tasa de aciertos, invalidar el token inmediatamente luego de la primera redirección, eliminar el proceso de redirecciones y/o poner en práctica mecanismos contra fuerza bruta en el servidor.

Conexiones Bluetooth

El Max de Lovense tampoco posee autenticación en sus conexiones BLE, con lo que puede realizarse un ataque de MitM para interceptar sus conexiones y enviar comandos de la misma forma en que se explicó anteriormente con el Jive. Los comandos para el control de los motores presentes en el dispositivo se pueden encontrar fácilmente entre el código de la aplicación, o pueden ser fácilmente interceptados al analizar el tráfico entre el juguete y el teléfono.

Actualizaciones de firmware

En cuanto a la actualización de firmware, Lovense Remote también posee algunas debilidades. El proceso de actualización de firmware comienza cuando la app envía al servidor un mensaje para chequear si existen actualizaciones disponibles con base en el tipo de dispositivo, su identificador y la versión actual. De ser afirmativo, el servidor responderá con una URL cifrada y el hash del archivo ZIP a descargar.

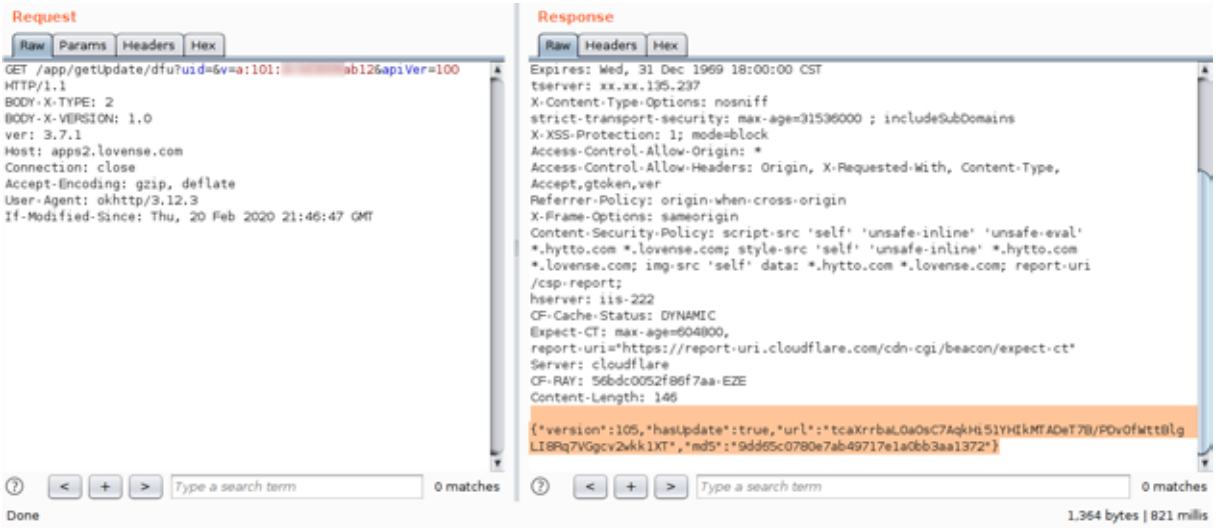

Figure 14// Petición para iniciar una actualización de firmware.

Sin embargo, dado que no se *verifica la autenticidad de los certificados* y que las claves de descifrado se encuentran almacenadas en el código de la aplicación, se vuelve relativamente sencillo para un atacante crear un script para interceptar los paquetes y redirigir a la víctima a su propia URL maliciosa.

MEJORES PRÁCTICAS PARA EVITAR ESTOS RIESGOS

El uso de juguetes sexuales que son controlados remotamente a través de aplicaciones está ganando popularidad como parte del concepto que se conoce como "sexnología": la combinación entre sexo y tecnología. Aunque estas prácticas hayan llegado para quedarse, no debemos olvidar los peligros que podrían acarrear para la privacidad e intimidad de los usuarios.

Para minimizar los riesgos asociados al uso de dispositivos sexuales inteligentes, recomendamos tener en cuenta los siguientes consejos sobre privacidad y sexting:

- Algunas aplicaciones ofrecen la posibilidad de controlar dispositivos localmente a través de BLE sin crear una cuenta de usuario. Si no planeas permitir que otros usuarios controlen tu dispositivo de forma remota a través de Internet, evita estas aplicaciones.
- En lo posible, evitar compartir fotos o videos en los que puedas ser identificado y no publicar en Internet los tokens de control remoto.
- Evitar registrarse en las aplicaciones sexuales con un nombre o correo electrónico oficial o que permita identificar a la persona; es decir, tratar de ser lo más anónimo posible. Considerar crear una nueva cuenta de correo para utilizar exclusivamente con estas apps.
- Leer siempre los términos y condiciones de las aplicaciones y sitios donde nos registramos o a los que se les envía información. Prestar especial atención a los apartados que hablan sobre la recolección de datos por parte de la empresa, así como de la forma en que los procesan. Fabricantes sin políticas de privacidad deberían ser evitados.

- Revisar estas políticas con frecuencia para comprobar si hay actualizaciones. Visitar periódicamente el sitio web del fabricante en busca de cambios que no hayan sido anunciados a través de la aplicación.
- Utilizar los juguetes sexuales inteligentes en un entorno protegido y evitar utilizarlos en lugares públicos o con circulación de personas (como hoteles).
- Mientras se utiliza el juguete, mantener la aplicación conectada al mismo dado que de esta manera se previene que se anuncie su presencia.
- Apagar el dispositivo y deshabilitar el Bluetooth mientras no esté en uso.
- Descargar las apps de control y probar sus funcionalidades antes de adquirir el dispositivo puede brindar al usuario un panorama de qué tan segura es la aplicación. Otra recomendación es utilizar los motores de búsqueda para averiguar si el modelo que se pretende adquirir ha tenido vulnerabilidades graves en el pasado, si existen parches para esas vulnerabilidades y si hay actualizaciones frecuentes por parte del desarrollador. Enviar un correo electrónico al departamento de soporte al cliente debería esclarecer cualquier duda al respecto.
- Proteger siempre los dispositivos móviles que se utilizan para controlar estos gadgets, mantenerlos actualizados e instalar una solución de seguridad en ellos.
- Proteger con contraseñas fuertes la red Wi-Fi hogareña que se utiliza para conectarse, algoritmos de cifrado seguros y actualizar con frecuencia el firmware del router.

Por último, si crees o sabes que el equipo que tienes en tu poder presenta vulnerabilidades graves, lo más recomendable es evitar utilizarlo de manera remota. En la medida de lo posible, deshabilitar el Bluetooth o las conexiones remotas mientras no están en uso.

PRÓXIMOS TEMAS A INVESTIGAR

Como habrá notado, para la realización de este análisis se tomaron en cuenta solo aplicaciones para Android, con lo cual aún resta por ver cuán vulnerables son las apps para dispositivos iOS. Además, vale la pena mencionar que existe una gran cantidad de modelos en los que, por obvias razones, no hemos podido analizar su firmware o su intercomunicación con las apps asociadas. En el futuro, nos gustaría adquirir nuevos equipos de diferentes marcas para llevar adelante una segunda parte de esta investigación. El estudio del firmware de los dispositivos en sí mismo mediante técnicas de fuzzing es otro de los aspectos que aún no han sido desarrollados por completo.

Por otro lado, las apps de citas y para ligar podrían quizás considerarse como los primeros desarrollos que surgieron en el camino hacia la naturalización de la sexualidad digitalizada, pero este camino no ha estado libre de obstáculos. Tinder, por ejemplo, ha tenido fallos que *permitieron obtener la geolocalización de un usuario*, o *crear perfiles falsos para conectar con otras personas* sin su consentimiento. A medida que el volumen de usuarios aumentó, las *estafas* se volvieron habituales en estas plataformas. Mientras tanto, nuevas apps han ido surgiendo con el paso del tiempo y hoy el abanico de opciones para elegir es variado. Un análisis sistemático de este tipo de apps y sus vulnerabilidades para determinar cuán seguras son estas aplicaciones actualmente, permitiría complementar esta investigación sobre el estado de la sexualidad en medios digitales.

Por último, se han realizado diferentes avances en el diseño y creación de robots sexuales. Algunos modelos incluyen cámaras, micrófonos, y capacidad de análisis de voz basado en técnicas de inteligencia artificial. Basándonos en las *vulnerabilidades ya conocidas en entornos de robótica*, contactamos a fabricantes de robots sexuales pidiendo información sobre las características de seguridad que poseen, y los resultados no son nada alentadores. Muchos de estos robots se basan en teléfonos con Android que manejan sus sensores como lo harían dispositivos periféricos, y añaden capacidades de Inteligencia Artificial a través de aplicaciones. Estas apps no están disponibles en tiendas oficiales y, por tanto, las

actualizaciones son enviadas a los usuarios vía correo electrónico, lo cual genera importantes agujeros de seguridad. El *uso de estos robots como reemplazo de los trabajadores sexuales* en burdeles ya es una realidad, por lo que un estudio de sus limitaciones desde la perspectiva de la seguridad de la información es imperativo para impulsar el desarrollo seguro de estas nuevas tecnologías.

AGRADECIMIENTOS

Nos gustaría agradecer a WOW Tech Group y a Lovense por su cooperación en el tratamiento de los problemas reportados.

A continuación, publicamos las declaraciones oficiales de los fabricantes en relación con nuestra divulgación, traducidas del inglés.

WOW Tech Group:

Dada la naturaleza íntima de nuestros productos, la privacidad y seguridad de los datos de nuestros clientes es de suma importancia para WOW Tech Group. Nos tomamos muy en serio los informes y hallazgos de fuentes externas sobre posibles vulnerabilidades. Por eso también estamos en estrecho contacto con ESET acerca de los resultados de su investigación y estamos agradecidos por su trabajo.

Tuvimos la oportunidad de parchear las vulnerabilidades antes de la presentación y publicación de este informe y, desde entonces, hemos actualizado la aplicación We-Connect para solucionar los problemas que se describen en este informe. En detalle, hemos agregado un tiempo de espera cada vez que se ingresa un pin incorrectamente para reducir el riesgo de ataques automatizados. Hemos actualizado la aplicación para eliminar metadatos multimedia antes de la transmisión y eliminar archivos al final de cada sesión de chat–no se almacenan ni guardan metadatos dentro de la aplicación o en nuestros servidores. ESET ya probó estas mejoras y se descubrió que eliminaron los problemas de seguridad anteriores.

Además, realizamos auditorías de seguridad regulares y abordamos los problemas de seguridad a medida que se descubre que cumplen con las mejores prácticas y estándares de seguridad actuales. Con la ayuda de expertos externos en seguridad y privacidad, nos esforzamos por fortalecer continuamente nuestras medidas de protección y seguridad de datos para ofrecer productos seguros a nuestros clientes.

Lovense:

Dando prioridad a la salud y la seguridad de nuestros usuarios, Lovense trabaja incansablemente para mejorar la ciberseguridad de sus productos y soluciones de software. Gracias a la cooperación productiva con el laboratorio de investigación de ESET pudimos detectar algunas vulnerabilidades que se han eliminado con éxito. Lovense continuará cooperando con investigadores de ciberseguridad para garantizar la máxima seguridad para todos los usuarios de los productos Lovense.

CRONOLOGÍA DE LOS HALLAZGOS

Tercer cuatrimestre de 2019 – Comenzamos a probar Jive de We-Vibe y el Max Masturbator de Lovense.

Jive

19 de junio de 2020 – Enviamos un correo a WOW Tech Group para reportar las vulnerabilidades.
24 de junio de 2020 – Enviamos un correo a WOW Tech Group para reportar las vulnerabilidades.
22 de julio de 2020 – Enviamos un correo a WOW Tech Group para reportar las vulnerabilidades.
22 de julio de 2020 – Primera respuesta por parte de WOW Tech Group.
24 de julio de 2020 – WOW Tech Group reconoció las vulnerabilidades.

3 de agosto de 2020 – Lanzamiento de la versión 4.4.1 de We-Connect corrige los problemas de metadatos y en el PIN de bloqueo.

Lovense Max

19 de junio de 2020 – Enviamos un correo a Lovense para reportar las vulnerabilidades.

24 de junio de 2020 – Enviamos un correo al equipo de seguridad de Lovense para reportar las vulnerabilidades.

30 de junio de 2020 – El reporte de la vulnerabilidda fue reconocido por Lovense.

27 de julio de 2020 – Todas las vulnerabilidades discutidas en este whitepaper fueron reparadas en la versión 3.8.6 de la app Lovense Remote y está disponible en la tienda Google Play.

10 de octubre de 2020 – Lovense continúa trabajando en nuevas funciones de privacidad para su app.

ACERCA DE ESET

Por más de 30 años, *ESET®* ha estado desarrollando soluciones y servicios de seguridad informática líderes en la industria para las empresas y los consumidores de todo el mundo. Con soluciones que abarcan desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases, los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología a pleno. ESET brinda protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Las amenazas en evolución requieren que la empresa de seguridad de TI también esté en constante evolución. Gracias al respaldo de sus Centros de Investigación y Desarrollo en todo el mundo, ESET es la primera empresa de seguridad de TI en ganar *100 premios VB100 de Virus Bulletin*, por detectar todo el malware in-the-wild sin interrupciones desde el año 2003. Para obtener más información, visite *www.eset.com/latam* o síganos en *LinkedIn*, *Facebook* y *Twitter*.