Análisis de la vulnerabilidad en iOS Mail. Recomendaciones y buenas prácticas

Abstract: tras la detección de una serie de vulnerabilidades Zero-Day en la aplicación de correo nativa de iOS, que podrían permitir a los atacantes la ejecución de código de forma remota a través del envío de un correo electrónico, se analizan a continuación las características de dicha vulnerabilidad y se recogen una serie de recomendaciones.

El día 20.05.2020 Apple hizo pública la versión 13.5 de iOS que corregía distintos problemas de seguridad entre los que se encontraba la vulnerabilidad 0-Click de la aplicación Mail iOS. Esta información se incluye en el apartado 6 "SERVICIO DE SOPORTE DE VULNERABILIDADES". Desde la publicación de las nuevas versiones iOS 13.5 y 12.4.7 se incluye una API de exposición a la COVID-19 analizada en el apartado 7 "ANÁLISIS DE LA API DE EXPOSICIÓN AL COVID-19".

El 01.06.2020 Apple lanza una nueva versión 13.5.1 que se evalúa en el apartado 8 "DETALLES DE LA ACTUALIZACIÓN VERSIÓN 13.5.1" del presente documento.

Contenido:

1 ANTECEDENTES

El uso de dispositivos móviles y tabletas se ha convertido en un mecanismo habitual de operación. Muchas de las tareas que tradicionalmente se habían realizado desde portátiles u ordenadores de sobremesa, se realizan ahora desde este tipo de dispositivos. Dos ejemplos bastante habituales se pueden encontrar en la navegación por Internet o en la lectura de correo electrónico.

Si bien en el caso de las respuestas a correos electrónicos es bastante frecuente que se lleven a cabo aún desde un ordenador, especialmente aquellos que son densos o críticos, no es así la operativa de lectura de estos, que es más habitual realizarla en un dispositivo móvil. Esto se debe a que lo que se busca fundamentalmente es la inmediatez del proceso y un acceso ágil, funcionalidades que sí aportan estos dispositivos.

Es también bastante habitual la tendencia a pensar que los dispositivos móviles tienden a ofrecer bastante seguridad, especialmente si no se realiza con ellos actividades potencialmente peligrosas como la ruptura de su seguridad o el desbloqueo de la

configuración de fábrica para instalar aplicaciones o funciones no soportadas por el fabricante.

También se asume que, con un limitado número de aplicaciones en el dispositivo, y siendo estas controladas, la posibilidad de impacto es siempre menor. Pero, ¿qué sucede cuando una aplicación nativa del propio dispositivo es vulnerable?

El día 20.04.2020 se hizo pública la explotación de una vulnerabilidad que podría estar afectando a los dispositivos con sistema operativo tipo iOS, fundamentalmente iPhone e iPad. Dicha vulnerabilidad afectaría a una de sus aplicaciones fundamentales: la aplicación Mail que presenta dichos dispositivos y que es bastante empleada al ser nativa y permitir conectarse a diversas plataformas como MS Exchange Server, Office 365 o Gmail.

Aunque la publicación de dicha vulnerabilidad es reciente, los análisis que se están efectuando inciden en pensar que la explotación podría haberse estado produciendo desde el año 2018, entrando dentro de la categorización de vulnerabilidad tipo Zero-Day.

2 AFECTACIÓN Y VECTOR DE ATAQUE

El análisis llevado a cabo y las verificaciones efectuadas por el equipo de ciberseguridad del CCN-CERT habrían permitido determinar que en la actualidad todas las versiones de iOS desde la 6 a la 13.4.1, se verían afectadas por dicha vulnerabilidad.

La vulnerabilidad tendría las siguientes características:

- La vulnerabilidad permitiría llevar a cabo a un atacante la ejecución de código remoto en el contexto de la aplicación nativa de correo electrónico del dispositivo.
- El vector de ataque consistiría en el envío de correos electrónicos especialmente construidos para la explotación de la vulnerabilidad y que tendría como característica el consumo de memoria RAM, aunque los mensajes no fueran particularmente grandes, debido a las características que podrían contener determinados ficheros adjuntos anexos al mismo.
- En función de la versión iOS, la afectación se llevaría a cabo a través de la metodología Zero-click, es decir sin la intervención del usuario y solo con la previsualización de los correos electrónicos. Este hecho se ha constatado en las versiones de iOS 13, mientras que en versiones previas requería de la intervención del usuario mediante la apertura del correo malformado, aunque la explotación no precise realizar ninguna otra acción adicional como clicar en ningún enlace o la apertura de los archivos adjuntos.
- Aunque evidentemente la implementación de una versión superior de iOS conlleva de forma natural una mejora en seguridad, en este caso se considera una situación más desfavorable. No obstante, en la lógica y en un uso convencional de

la aplicación de correo electrónico conllevaría las mismas consecuencias que para versiones iOS 13, ya que implica la necesidad de interacción con los correos, fundamentalmente su apertura y por lo tanto la afectación para versiones iOS 12 y anteriores.

- La capacidad de postexplotación de la vulnerabilidad, si esta se ha producido, permitiría a un atacante:
  - Tener acceso al contenido del dispositivo en el contexto de la aplicación, incluyendo con ello todos los permisos que dicha aplicación tuviera, tales como acceso a contactos, interacción con otras aplicaciones, etc.
  - Manipular la aplicación para permitir reenvíos de contenido no visibles por el usuario o realizar inyecciones de código para manipulación de correos o contenido.
  - Tener acceso a información de gestión de la aplicación, incluyendo la cuenta de correo electrónico o la contraseña empleada para garantizar el acceso.
- Inicialmente, el compromiso completo del dispositivo no se contempla con la explotación única de dicha vulnerabilidad, ya que el diseño de la arquitectura iOS circunscribe la problemática al contexto de la aplicación principalmente.
- Las evidencias de afectación no son fáciles de identificar actualmente, y sin claros indicadores de compromiso que permitan verificar si un dispositivo ha podido ser o no afectado.

  La problemática en algunas circunstancias cursa con el cierre inesperado de la aplicación de correo, con la ralentización de esta o con una mala visualización de los correos electrónicos. Sin embargo, cuando la afectación se ha producido, puede que las consecuencias posteriores no sean visibles por parte del usuario.

3 POTENCIALIDAD DEL ATAQUE

Hasta la fecha de publicación de la vulnerabilidad por parte de la organización ZecOps, se estima que serían pocas las agencias u organizaciones que estarían en disposición de conocer y aprovechar dicha vulnerabilidad. Aunque es cierto que potencialmente la vulnerabilidad de día cero se podría estar explotando desde el año 2018, el nivel de afectación podría haber sido limitado.

Sin embargo, a raíz de la publicación, se han llevado a cabo estudios que han revelado donde se encontrarían los desencadenadores (*trigger*), la funciones de truncado y llamadas que permitirían llevar a cabo la explotación de la vulnerabilidad. Aunque ya se ha identificado claramente un mecanismo de explotación de la vulnerabilidad a través de funciones de truncado para un desbordamiento de buffer, se están abriendo nuevas investigaciones que permitirían a través de otras acciones hacer también efectivas la explotación.

Estos estudios bastante detallados, e incluso con pruebas de concepto bajo determinadas condiciones, permitirían que un significativo número de personas tuvieran acceso a material antes no conocido, para llevar a cabo la construcción de correos malformados que aprovecharan la debilidad existente.

Por lo tanto, es previsible tal y como ha sucedido en otra tipología de campañas, que se empiece a producir una escalada de envío de correos que aprovecharían la vulnerabilidad publicada con diversos fines.

4 ELEMENTOS NO AFECTADOS

Para circunscribir la problemática, es necesario incidir en algunas pautas descritas previamente:

- La vulnerabilidad queda limitada a la aplicación nativa de correo de sistemas iOS. Es decir, aplicaciones tales como Outlook for iOS o email for Google para acceso a Gmail, no se verán afectadas por dicha vulnerabilidad.
- La vulnerabilidad no afecta al sistema operativo MacOS, siendo por lo tanto solo aplicable sobre dispositivos con versiones iOS.

5 CONCLUCIONES Y RECOMENDACIONES

Atendiendo a las circunstancias anteriormente descritas, se destacan las siguientes conclusiones:

- La vulnerabilidad se limita a la aplicación de Mail de sistemas IOS, nativa en la versión para dispositivos del fabricante Apple. Por lo tanto, no serían vulnerables otras aplicaciones de correo electrónico sobre dispositivos con sistema operativo iOS: iPhone o iPad.
- El vector de ataque se produce a través de correo malformado, que aprovecharía debilidades en el comportamiento de la aplicación de correo electrónico. Dichas debilidades se producen en el tratamiento de los componentes S-MIME a través de determinados procesos de truncado, aunque se están abriendo nuevas vías potenciales para la explotación de la vulnerabilidad.
- Es probable que la explotación se pueda estar dando desde el año 2018, aunque con un alcance limitado y altamente dirigido. No obstante, es muy probable que el ataque se popularice tras la publicación de la vulnerabilidad, debido fundamentalmente a la proliferación de análisis y publicación de resultados detallados para llevar a cabo la explotación efectiva.

Como resultado final, se estiman las siguientes recomendaciones:

- Cuando el fabricante haya hecho pública la versión definitiva (no BETA) que resuelve la vulnerabilidad, deberían actualizarse los dispositivos afectados. Cabe

decir que no todos los dispositivos podrán instalar dicha versión, debido a que desde la salida de la versión 13.0 dicha nueva rama del Sistema Operativo no está disponible para todos los modelos del fabricante Apple.

- Hasta la publicación de la actualización de seguridad, todos aquellos dispositivos que empleen la aplicación Mail de iOS deberían dejar de utilizarla empleando en su lugar aplicaciones alternativas como Outlook o email de Google para G-Mail.

  Para ello, se recomienda desactivar temporalmente la/las cuentas de correo que usan la *app* Mail, siguiendo el procedimiento que se indica:

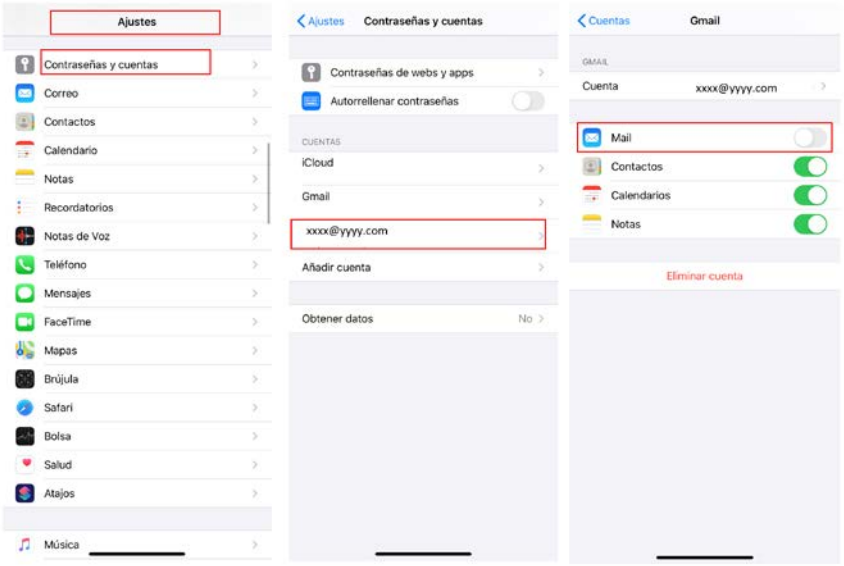

Ilustración 1.- Desactivación cuenta Mail

- Bloquear la adición de nuevas cuentas en el dispositivo móvil estableciendo una restricción, concretamente a través de "Ajustes - Tiempo de uso - Contenido y privacidad - [Permitir cambios] Cambios en la cuenta".

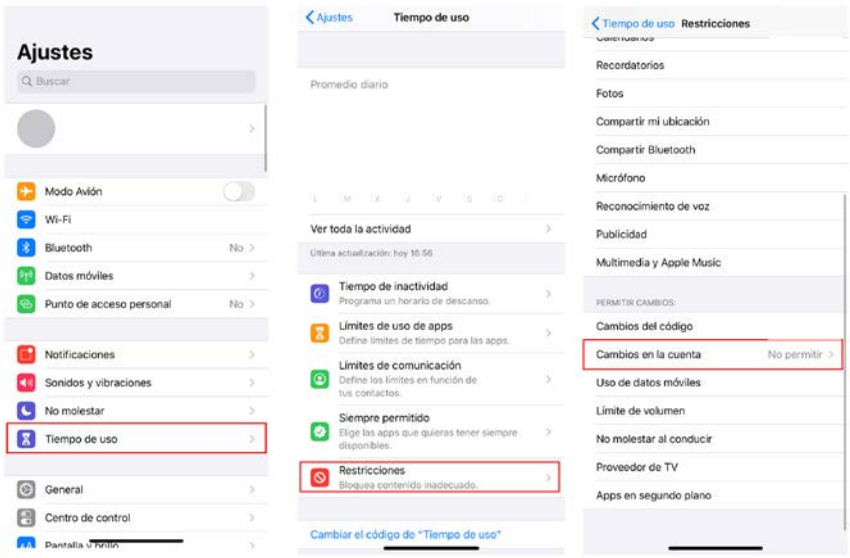

Ilustración 2.- Bloqueo activación de cuentas

- Como opción alternativa, se podría desinstalar temporalmente la *app* Mail de iOS o iPadOS manteniendo los datos asociados, mediante el menú "Ajustes - General - Almacenamiento del iPhone - Mail - Desinstalar app".

  De este modo, se conservarán los datos de la cuenta de correo en el dispositivo móvil y, al reinstalar la *app* una vez se disponga de la actualización, se podrán recuperar. Sin embargo, mientras no se disponga de la *app* Mail, no será posible acceder a los datos de correo descargados localmente.

  En cualquier caso, se recomienda disponer de una copia de seguridad del dispositivo móvil, y del buzón de correo de la cuenta en el servidor de correo.

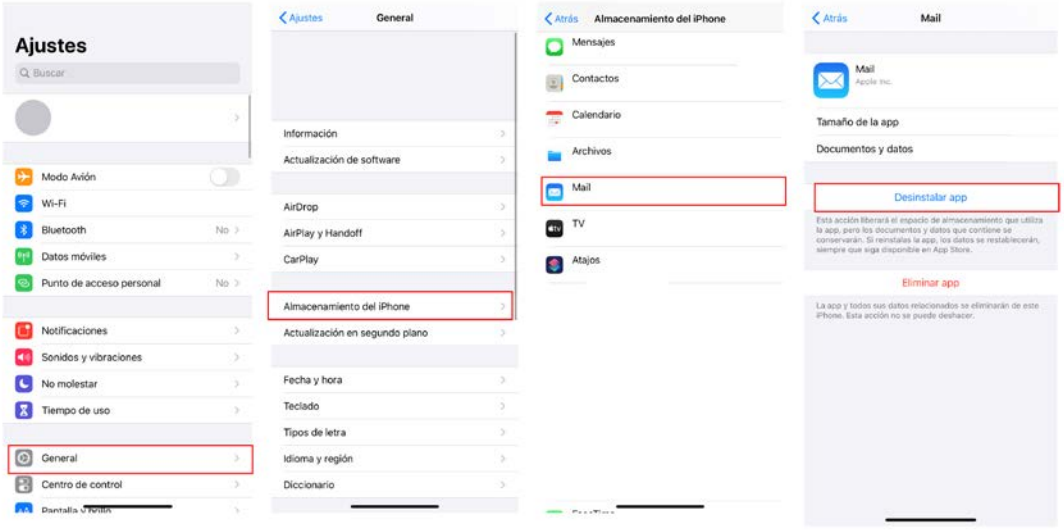

Ilustración 3.- Desinstalación temporal cuenta app Mail

- En aquellos dispositivos en los que se haya constatado la existencia de evidencias de afectación, sería recomendable llevar a cabo un proceso de evaluación para determinar hasta qué punto han sido afectados. Ante cualquier indicio de problema podrían ser aconsejables las siguientes acciones:
  - Restauración a condiciones de fábrica del dispositivo.
  - Utilización del dispositivo sin el empleo ni configuración de la aplicación nativa de Mail, utilizando es su lugar una aplicación alternativa para el tratamiento de correo electrónico.
  - Cambio de credenciales empleadas para el acceso de correo, para limitar el hecho de que dicha información pudiera estar en manos de terceros.
- En el caso de las organizaciones donde no sea factible dejar de hacer uso de la aplicación nativa Mail, se deberán implementar mecanismos de análisis o monitorización bien a través de tecnologías Mobile Device Management (MDM) o aquellas para la monitorización de terminales o uso de correo electrónico.

- Debe tomarse en cuenta que uno de los indicadores más claros que permitirían establecer una potencial explotación de la vulnerabilidad, consistiría en el aumento significativo de memoria RAM vinculado a dicha aplicación.
- Ante circunstancias de potencial explotación de vulnerabilidad de la aplicación Mail, es bastante previsible que la aplicación incremente el nivel de uso de datos que puede llegar a evaluarse a través de herramientas de gestión centralizada tipo MDM.

  Así ante un ataque efectivo, es bastante previsible que en consecuencia se produzca una exfiltración de correos a cuentas externas que podrán ser evaluadas o monitorizadas desde los *Mail Transfer Agent* (MTA) de correo electrónico de la organización, a la vez que se puede evaluar posibles incrementos en el uso de datos asociados a la aplicación.
- Sería también aconsejable, en tanto en cuanto no pueda dejar de utilizarse la aplicación Mail, que se limiten o monitoricen las acciones de dicha aplicación para el acceso a funciones o elementos del dispositivo, tales como cámara, micrófono, llamadas o similares. Aunque no se limita la problemática, se minimiza un potencial impacto de aprovechamiento de uso no controlado de la aplicación por parte de un tercero.
- Actualmente, solo se disponen de pequeñas muestras dentro de los potenciales mecanismos de *payload* para realizar la explotación (https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/#), que si bien reducen la superficie de exposición a la vulnerabilidad no cubren toda la posible casuística (valores S-MIME, en el cuerpo, en referencias HTML, en ficheros anexos, ...).

  Aun así, siempre es recomendable que en los equipos perimetrales dedicados a la protección del correo se pongan reglas más estrictas o activar la parte de protección al CEO que tienen FortiMail y Cisco.

En definitiva, las organizaciones deberían ir evaluando las nuevas informaciones técnicas que vayan siendo publicadas y los posibles vectores de ataque. Es bastante probable que con la evolución y el conocimiento en las técnicas de explotación se vayan generando reglas de evaluación, bien en los sistemas MTA de protección de correo electrónico o bien en los sistemas de prevención de intrusiones, que permitan detectar correos maliciosos a partir del *payload* capaces de llevar a cabo la explotación en la aplicación Mail.

6 SERVICIO DE SOPORTE DE VULNERABILIDADES

Como parte del servicio de monitorización de vulnerabilidades que el CCN-CERT presta para el análisis, notificación y seguimiento de aquellas vulnerabilidades más críticas y

que impacten especialmente en las tecnologías empleadas en el sector público, se recogen los resultados de los análisis realizados desde el día 20.04.2020 que se hizo pública la explotación.

Fuentes consultadas:

El seguimiento realizado por el servicio de soporte de vulnerabilidades se ha centrado en los siguientes entornos:

- 10 Blogs especializados.
- 33 páginas Webs.
- Pruebas de concepto.
- 181 Redes sociales.
- Fuentes oficiales del fabricante.

De la información obtenida se han obtenido los siguientes resultados:

- Resultados totales: 224
- Resultados descartados: 201
- Resultados que aporten nueva información: 2
- Resultados con información falsa: 0
- Pruebas de concepto: 0 (pendiente de publicación).

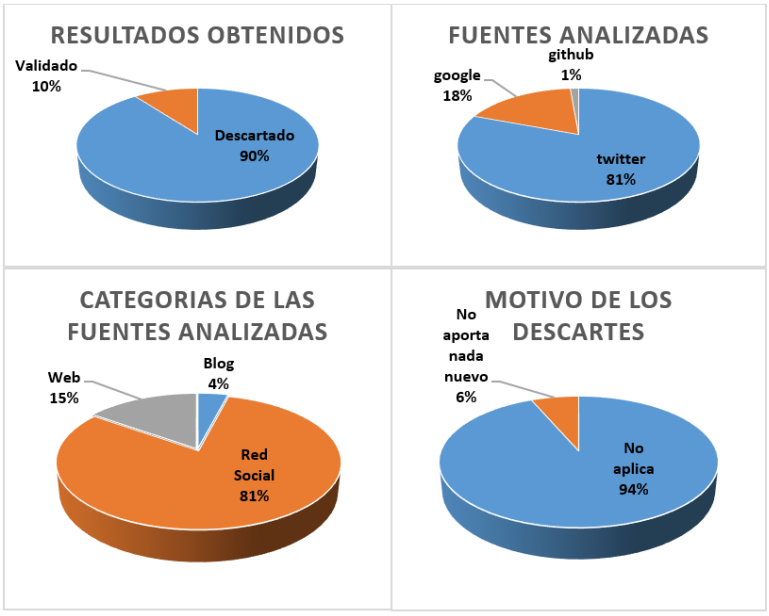

Ilustración 4.- Resultados fuentes consultadas

Ampliación de la Afectación:

Inicialmente la vulnerabilidad iOS Mail afectaba a todos los dispositivos con una versión de iOS comprendida entre la versión 6 y la 13.4.1, pero el día 9.05.2020 los

descubridores de la vulnerabilidad redactaron una nueva entrada en su blog (https://blog.zecops.com/vulnerabilities/seeing-maildemons-technique-triggers-and-a-bounty/) en la que se demostraba que la vulnerabilidad afectaba a versiones de iOS desde la versión 3.1.3. Esto hace que la afectación de la vulnerabilidad se amplíe desde la versión 3.1.3 hasta la versión 13.4.1.

Lanzamiento de la versión iOS 13.5:

El día 20.05.2020, Apple lanzó la versión iOS 13.5 (https://support.apple.com/en-us/HT201222). Esta última actualización incluye la corrección de la vulnerabilidad iOS Mail.

Apple no ha publicado aún los detalles de la actualización, pero los investigadores han confirmado que esta versión corrige la vulnerabilidad (https://twitter.com/ZecOps/status/1263359839821914112?s=20). Por el momento, se desconoce si se harán públicas pruebas de concepto o *exploits*.

La versión 13.5 está disponible para los siguientes dispositivos:

- iPhone a partir de la versión 6s.
- iPad Air a partir de la versión 2.
- iPad mini a partir de la versión 4.
- iPod touch séptima generación.

Mejoras asociadas a la versión 13.5:

Además de la corrección de la vulnerabilidad, la versión iOS 13.5 incluye nuevas mejoras. A continuación, se listan algunas de ellas:

- Mejora la velocidad al acceder al campo de código en dispositivos con Face ID cuando el usuario lleva una mascarilla.
- Contiene la interfaz API “Notificaciones de exposición” que agrega compatibilidad con las *apps* de rastreo del contacto de COVID-19 de las autoridades de salud pública.

Lanzamiento de la versión iOS 12.4.7:

Coincidiendo con la salida de la versión 13.5 de iOS, Apple lanzó la versión 12.4.7 (https://support.apple.com/en-hk/HT201222). El día 21.05.2020, los descubridores de la vulnerabilidad confirmaron que esta versión, al igual que la versión 13.5, corrige la vulnerabilidad iOS Mail.

La versión 12.4.7 está disponible para los siguientes dispositivos:

- iPhone 5s.
- iPhone 6s.
- iPhone 6 Plus.

- iPad Air.
- iPad mini 2.
- iPad mini 3.
- iPod touch sexta generación.

Para actualizar a la versión iOS 13.5, se deben seguir los siguientes pasos:

1. Desde el dispositivo diríjase a “Ajustes”.
2. Acceda a “General” > “Actualización de software”.
3. Tras el tiempo de carga podrá descargar la actualización.

Se desconoce si Apple va a sacar una versión que corrija el fallo en los dispositivos para los que no está disponible esta actualización, por lo que se aconseja aplicar las recomendaciones incluidas en el apartado 5 “CONCLUSIONES Y RECOMENDACIONES” del presente documento.

El servicio de soporte de vulnerabilidades continuará con el seguimiento y la monitorización de la vulnerabilidad y comunicará a los organismos adheridos al servicio cualquier nueva información que pueda surgir al respecto.

7 ANÁLISIS DE LA API DE EXPOSICIÓN AL COVID-19

Descripción de la API:

Apple y Google han colaborado para desarrollar una API de exposición que ponen a disposición de los servicios públicos de salud de todo el mundo y que permite el rastreo de contactos de riesgo en relación con la COVID-19.

Funcionamiento:

Tal y como se describe en la documentación aportada por estas empresas en su referencia oficial, esta API funciona usando identificadores numéricos generados de manera aleatoria para identificar a cada usuario de manera anónima. Estos identificadores además varían cada 20 o 30 minutos para evitar que puedan ser rastreados.

La API realiza un envío de paquetes, mediante la tecnología *bluetooth*, con este identificador a los dispositivos cercanos que a su vez muestran su identificador al dispositivo emisor. Esta información se guarda de manera segura y no se utiliza hasta que se notifica un caso positivo de COVID-19.

Una vez que un usuario notifica que es positivo mediante un test a través de una aplicación que integre la API, se envía esta información también de manera anónima y desde ese momento a cualquier persona que haya tenido contacto con uno de los identificadores aleatorios asociados a ese usuario. Las personas que hayan estado en contacto al ser notificadas podrán tomar las medidas oportunas.

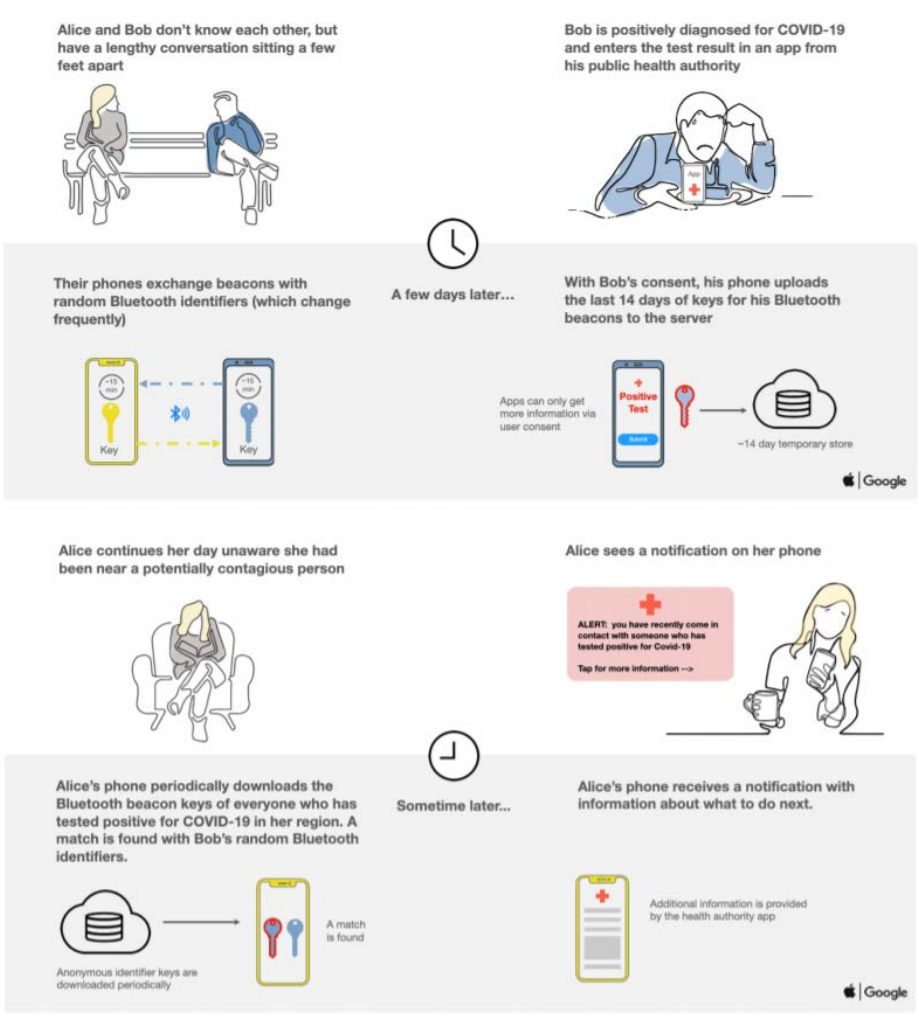

Ilustración 5.- Funcionamiento de la API de exposición a la COVID-19

Consideraciones de seguridad:

Tal y como se indica en la documentación de los fabricantes, la API no almacena ningún dato de carácter personal, de ubicación o de uso.

Google y Apple no venderán los datos obtenidos a través de API a terceros. Además, toda aquella organización de salud pública que quiera hacer uso de la API deberá de cumplir una serie de requisitos y políticas de privacidad.

El cifrado y almacenamiento de información se realiza en todo momento en el propio dispositivo, salvo en caso de contagio, que se envía el conjunto de identificadores aleatorios que identifican al dispositivo.

La API no viene activada en ningún caso por defecto y se debe activar manualmente. De la misma manera se puede desactivar en cualquier momento.

Criptografía en uso:

Las funciones criptográficas usadas por la API son las siguientes:

- HKDF (estándar IETF RFC 5869, SHA-256).

- AES-128.
- AES-CTR (AES-128 Counter Mode).
- CRNG (Generación de números aleatorios).

Todas estas funciones están consideradas como seguras hasta la fecha.

Implementación de API:

Existen varios recursos que pueden ser de ayuda a la hora de implementar esta API:

Repositorio de GitHub con una aplicación de ejemplo:

- https://github.com/google/exposure-notifications-android

Documentación de la API:

- https://static.googleusercontent.com/media/www.google.com/es//covid19/exposurenotifications/pdfs/Android-Exposure-Notification-API-documentation-v1.3.2.pdf

Implementación de código abierto del servidor:

- https://github.com/google/exposure-notifications-server

Otros datos de interés:

Relacionado con la API de exposición lanzada por Google y Apple, en España diferentes comunidades autónomas van a ejecutar proyectos que harán uso de este tipo de funcionalidades:

- La comunidad autónoma de Canarias acogerá un proyecto piloto de una aplicación móvil de rastreo de contagios por COVID-19 que se desarrollará a nivel europeo, y en el que ya están trabajando el Gobierno canario y el Gobierno central, a través de las Consejerías de Sanidad, de Administraciones Públicas, de Justicia y de Seguridad y del Ministerio de Asuntos Económicos y Transformación Digital.

  (https://www.lavozdelanzarote.com/articulo/canarias/canarias-acogera-proyecto-piloto-rastreo-contagios-covid-19-espana-traves-app-movil/20200520203407150832.html)

- Generalitat valenciana: aplicación de rastreo de contagios por COVID-19 basada en DP3T. (https://www.xatakamovil.com/aplicaciones/asi-funciona-app-rastreo-contagiados-coronavirus-basada-dp3t-que-se-esta-desarrollando-para-valencia)

- Artículo que describe la API gráficamente y que habla sobre la posibilidad de que en España se use para la detección de posibles contagios por contactos de riesgo además de otra posible alternativa a la misma.

  (https://www.lavanguardia.com/vida/20200522/481318031656/espana-explora-una-app-para-rastrear-contagios-por-movil.html)

Referencias:

- https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf
- https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf
- https://www.google.com/covid19/exposurenotifications/

8 DETALLES DE LA ACTUALIZACIÓN VERSIÓN 13.5.1

Tal y como Apple describe en el mensaje de actualización y que los usuarios pueden ver en el gestor de actualizaciones de los dispositivos para los que está disponible la actualización, la versión 13.5.1 de iOS informa de actualizaciones de seguridad importantes.

Ilustración 6,- Detalles de la actualización iOS 13.5.1

Además, en los contenidos de seguridad incluidos en esta versión Apple indica que la actualización corrige una vulnerabilidad en el *kernel* que permite la ejecución de código arbitrario. Esta vulnerabilidad tiene asociado el código CVE-2020-9859.

CVE-2020-9859

La vulnerabilidad CVE-2020-9859 fue descubierta por un equipo de investigadores llamados unc0ver Team. Esta vulnerabilidad permite la ejecución de código arbitrario con privilegios de *kernel*.

Gracias a la explotación de esta vulnerabilidad, la herramienta unCover desarrollada por los investigadores permite realizar *jailbreak* a todos los dispositivos que estuvieran afectadas por la misma. El *jailbreak* permite acceder a opciones que el fabricante no facilita en las versiones de fábrica, haciendo que el sistema sea más configurable y personalizable. Por el contrario, liberar el sistema operativo de las restricciones de su fabricante hace que sea más inseguro y potencialmente más vulnerable.

El día 01.06.2020 uno de los investigadores del equipo unCover confirma que la versión 13.5.1 de iOS corregía la vulnerabilidad CVE-2020-9859 que permitía realizar el *jailbreak*, tal y como se puede ver en el siguiente tweet:

- https://twitter.com/Pwn20wnd/status/1267530188964810752?s=20

La versión 13.5.1 de iOS está disponible para los siguientes dispositivos del fabricante:

- iPhone a partir de la versión 6s.
- iPad Air a partir de la versión 2.
- iPad mini a partir de la versión 4.
- iPod touch séptima generación.

Referencias:

- https://support.apple.com/en-us/HT211214