# Boletín de Ciberseguridad

Fecha de Publicación
25/10/2021 - N.º 19

Mes de octubre
11/10/2021 - 25/10/2021

Datasec

## Contenido

Introducción ..... 2
Apple parchea varios Zero-day que afectan a iPhone y Mac ..... 3
Vulnerabilidades múltiples en Google Chrome ..... 4
Estafa CryptoRom roba criptomonedas en Tinder ..... 6
Argentina: Filtración de datos del Registro Nacional de las Personas ..... 7
Adware, ataque de anuncios no deseados ..... 9
Estudio revela problemas de privacidad en Android ..... 11
Conclusiones ..... 13

## Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de las importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de octubre se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

### Vulnerabilidades múltiples en Google Chrome

Expertos en ciberseguridad alertan sobre vulnerabilidades críticas descubiertas recientemente en Google Chrome en sus versiones para Windows, Mac y Linux.
La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario en el contexto del navegador.

### Estafa CryptoRom roba criptomonedas en Tinder

Un informe de la empresa especializada en seguridad informática Sophos, reveló que ciberdelincuentes robaron 1.4 millones de dólares en criptomonedas a usuarios de iOS por medio de la aplicación para citas Tinder.
La estafa que comenzó en Asia se extendió a Estados Unidos y Europa.

### Estudio revela problemas de privacidad en Android

Un nuevo estudio llevado a cabo por investigadores universitarios del Reino Unido ha revelado una serie de problemas de privacidad relacionados con el uso de teléfonos inteligentes Android.
El estudio se centró en dispositivos Android de Samsung, Xiaomi, Realme y Huawei, y en LineageOS y /e/OS, dos forks de Android.


| | | |
|---|---|---|
|  | **Apple parchea varios Zero-day que afectan a iPhone y Mac** | CRÍTICO |



## Descripción

Apple ha lanzado una actualización de seguridad para corregir múltiples vulnerabilidades de día cero en dispositivos iPhone y Mac.

## Afectados

Apple iOS 14.0 a 15.0.2
iPadOS 14.0 a 15.0.2
macOS Big Sur
Safari

## Estado

Entre las Vulnerabilidades se encuentra:

- Una de las fallas, refiere a un problema de corrupción de memoria en el componente "IOMobileFrameBuffer" que podría permitir que una aplicación ejecute código arbitrario con privilegios del kernel.
- Zero-day corregido por Apple es un fallo de tipo "Use-After-Free" (UAF) que permite a WebKit ejecutar código arbitrario en un sitio web con contenido malicioso creado por un atacante.

- Otro zero-day, es una vulnerabilidad en CoreGraphics de tipo 'Integer overflow'. Permite también ejecutar código arbitrario al procesar un PDF con contenido malicioso.

## Remediación / Referencias

Se recomienda a los usuarios de Apple iPhone y iPad que actualicen la última versión para mitigar la vulnerabilidad de seguridad.

Para saber más:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00506-01/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30883
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860

| | | |
|---|---|---|
| Google Chrome | **Vulnerabilidades múltiples en Google Chrome** | CRÍTICO |

## Descripción

Expertos en ciberseguridad alertan sobre vulnerabilidades críticas descubiertas recientemente en Google Chrome en sus versiones para Windows, Mac y Linux.

La explotación exitosa de estas fallas podría permitir a un atacante ejecutar código arbitrario en el contexto del navegador.

## Afectados

Las versiones de Google Chrome afectadas son: 7.0.517.41 a 94.0.4606.71.

## Estado

Estos fallos son de alto impacto y permiten a los atacantes remotos ejecutar en el sistema objetivo un código arbitrario.

- La primera vulnerabilidad se debe a "un error de memoria luego de su liberación dentro de Garbage Collection en Google Chrome."
- La segunda falla existe a partir de un un desbordamiento del buffer Heap en Blink.
- La tercera vulnerabilidad se dio por un "error de límites de la memoria al procesar contenido HTML no confiable en WebRTC. "

Estos fallos resultan fáciles de explotar y no implica ninguna autenticación específica.

Actualmente no hay informes de que estas vulnerabilidades estén siendo explotadas.

**Remediación /Referencias**

Se recomienda a los usuarios que apliquen los parches de seguridad indicados por Google Chrome a la brevedad.

Para obtener más información al respecto:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00507-01/
https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html


| | | |
|---|---|---|
|  | **Estafa CryptoRom roba criptomonedas en Tinder** | IMPORTANTE |

## Descripción

Un informe de la empresa especializada en seguridad informática Sophos, reveló que ciberdelincuentes robaron 1.4 millones de dólares en criptomonedas a usuarios de iOS por medio de la aplicación para citas Tinder.

La estafa que comenzó en Asia se extendió a Estados Unidos y Europa.

## Afectados

Las víctimas son dueños de dispositivos iOS de Apple que poseen usuario en la aplicación de citas.

## Estado

Delincuentes informáticos hicieron uso de “Enterprise Signature”, un sistema para desarrolladores de software que ayuda a las organizaciones a probar nuevas aplicaciones iOS con usuarios seleccionados de iPhone antes de enviarlas a la App Store oficial de Apple para su revisión y aprobación.

Los atacantes crearon aplicaciones con apariencia de gestores de criptomonedas, para luego abrir perfiles falsos en Tinder y así convencer a las víctimas de instalar e invertir en una aplicación de comercio de criptomonedas falsa.

Los delincuentes podrían hacer más que solo robar inversiones falsas en criptomonedas, sino que también obtener el control remoto de los dispositivos de las víctimas recopilando datos personales, agregar o eliminar cuentas e instalar y administrar aplicaciones para otros fines maliciosos.

**Referencias**

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/10/cryptorom-estafas-de-citas-en-tinder.html
https://news.sophos.com/en-us/2021/10/13/cryptorom-fake-ios-cryptocurrency-apps/

| | | |
|---|---|---|
| | **Argentina: Filtración de datos del Registro Nacional de las Personas** | IMPORTANTE |

**Descripción**

La base de datos del Registro Nacional de la Personas (RENAPER) apareció filtrada y a la venta en la web. Dichos datos incluyen foto, nombres, apellidos, número de trámite de DNI, entre otros.

**Afectados**

Los afectados fueron personas físicas domiciliadas en Argentina.

**Estado**

RENAPER, organismo que depende del Ministerio del Interior Argentino, es el encargado de la emisión de las tarjetas de identificación nacionales a todos los ciudadanos argentinos que actualmente posee una base de datos que permite a las agencias gubernamentales acceder a la información personal de los ciudadanos.

Dicho organismo sufrió el mes pasado un hackeo a su base de datos que se dio a conocer debido a que un usuario de Twitter publicó imágenes de 44 personas, dentro de las que figuraban famosos y funcionarios públicos de Argentina, acompañadas de un texto en el que el ciberdelincuente advertía la venta de los datos.

A su vez, el atacante publicó un anuncio en un foro de hacking ofreciendo buscar los datos de cualquier habitante argentino a todos los compradores interesados.

Especialistas confirmaron que se trató de un usuario habilitado - o alguien que robó su clave- que se conectó a través de una cuenta VPN asignada al Ministerio de Salud, con usuario y contraseña.

Funcionarios niegan la filtración de los datos mientras que el ciberdelincuente afirma y amenaza con exponer los datos de 1 millón o 2 millones de personas a la vez que planea seguir vendiendo el acceso de estos datos a compradores interesados.

**Referencias**

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/10/robada-la-base-de-datos-completa-de.html
https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/


## Adware, ataque de anuncios no deseados

PREVENCIÓN

**Descripción**

El adware es un tipo de software malicioso que bombardea con incesantes anuncios emergentes, software gratuito, aplicaciones dudosas, entre otras, diseñado para desplegarse en la computadora o teléfono en el explorador.

**Afectados**

Cualquier usuario de la web que haga clic en los anuncios.

**Estado**

Adware, que proviene de “advertising” (publicidad) y “software” (programa), es un software no deseado diseñado para mostrar anuncios tanto en un explorador como en aplicaciones. Este puede ser malicioso o no, usándose para publicitar o también a menudo para dañar e interrumpir un sistema.

Al exhibirse a los usuarios anuncios publicitarios, el fabricante del Software obtiene ganancias a partir de los clics e impresiones en los anuncios.

El adware se considera un grayware, termino abarcador aplicado a un amplio rango de programas que son instalados en la computadora o teléfono de un usuario para dar seguimiento o reportar cierta información a un tercero.

**¿Cómo saber si tenemos instalado un adware?**

Hay determinadas señales que indican que un dispositivo está infectado con un adware:

- Aparecen anuncios emergentes de manera automática. Bombardeo de publicidad constante.
- Enlaces que redirigen a sitios no deseados o desconocidos.
- El navegador y el dispositivo tienden a estar más lentos de lo habitual.
- Instalación de programas y aplicaciones no deseadas.

Por estos comportamientos invasivos es que es el malware más fácil de detectar.

**Las maneras en que el adware se instala en los dispositivos pueden ser diversas:**

- Al instalar aplicaciones gratuitas, de prueba o al actualizar software que, por falta de atención, se acepta la instalación de un adware.
- Al ingresar a sitios web infectados.
- Al instalar extensiones en el navegador no confiables o desconocidas.

Contraseñas, datos personales, datos de tarjetas de crédito, datos de navegación, de consumo, entre otros, puede ser información obtenida por los adwares.

## Remediación / Referencias

Hay diferentes medidas para prevenir la propagación de adware.

Al navegar, siempre tomar precauciones.
Tener cuidado al descargar e instalar software nuevo, leer los términos y las condiciones, evitar abrir aplicaciones que vengan de fuentes desconocidas, usar antivirus y antimalware en la computadora y celular, mantener actualizado el sistema operativo y el navegador.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/10/15/que-es-adware-caracteristicas/

| android | Estudio revela problemas de privacidad en Android | PREVENCIÓN |
|---|---|---|

## Descripción

Un nuevo estudio llevado a cabo por investigadores universitarios del Reino Unido ha revelado una serie de problemas de privacidad relacionados con el uso de teléfonos inteligentes Android.

El estudio se centró en dispositivos Android de Samsung, Xiaomi, Realme y Huawei, y en LineageOS y /e/OS, dos forks de Android.

## Afectados

Usuarios de dispositivos Android.

## Estado

El estudio encontró que "incluso con una configuración mínima y cuando el teléfono está inactivo, las variantes de Android específicas del fabricante transmiten cantidades considerables de información" no sólo con los fabricantes de dispositivos, sino también se comparte con terceros como, por ejemplo, Facebook, Linkedin y Microsoft.

Algunos de los datos compartidos incluyen: identificadores persistentes, uso detallado de aplicaciones, información telemétrica.

En una de las tablas que se presentan en el estudio, Google aparece en casi todas partes como el extremo receptor de los datos.
El mismo estudio explica que los usuarios de Android no disponen de una opción de "exclusión" para elegir como medida de mitigación contra este tipo de recogida de datos.
Algunos proveedores de smartphones incluyen a veces aplicaciones de terceros. Esto significa que estas apps de terceros realizan la recogida de datos de forma silenciosa, por lo que no importa que el propietario del dispositivo no haga uso de ellas. Y, lo que es más, es que no se pueden eliminar.

"En el caso de algunas de las aplicaciones integradas en el sistema, como miui.analytics (Xiaomi), Heytap (Realme) e Hicloud (Huawei), los investigadores descubrieron que los datos cifrados pueden descifrarse en ocasiones, lo que supone un riesgo para los ataques de tipo Man-in-the-Middle (MitM)."

Lo que es interesante mencionar, tal y como subrayan los investigadores, es el hecho de que incluso si se restablecen los identificadores publicitarios de la cuenta de Google en Android, esto no impide que el sistema de recopilación de datos haga que el nuevo identificador vuelva a vincularse al mismo dispositivo.

"Un portavoz de Google ha declarado lo siguiente sobre las conclusiones del estudio:

Aunque apreciamos el trabajo de los investigadores, no estamos de acuerdo en que este comportamiento sea inesperado: así es como funcionan los smartphones modernos.
Como se explica en nuestro artículo del Centro de ayuda de los servicios de Google Play, estos datos son esenciales para los servicios básicos del dispositivo, como las notificaciones push y las actualizaciones de software, en un ecosistema diverso de dispositivos y versiones de software.
Por ejemplo, los servicios de Google Play utilizan los datos de los dispositivos Android certificados para respaldar las funciones principales del dispositivo. La recopilación de información básica limitada, como el IMEI de un dispositivo, es necesaria para ofrecer actualizaciones críticas de forma fiable en todos los dispositivos y aplicaciones Android."

## Referencias

Para acceder al estudio completo:
https://www.scss.tcd.ie/Doug.Leith/Android_privacy_report.pdf
https://blog.segu-info.com.ar/2021/10/informe-sobre-datos-recogidos-por.html

## Conclusiones

Cada día somos participes de que la información es el oro de esta generación; cada día observamos como en todas las situaciones, sea estado o privados, tenemos fugas de datos que son tanto a propósito (como lo que puede pasar con las empresas tecnológicas Chinas hoy en día), o como aquellos que quieren evitar las fugas de datos y no lo logran (como es el caso de Argentina). Nadie está a salvo y somos conscientes de que la seguridad es otra de esas carreras que nos llevará al éxito o fracaso.

Poder medir y actuar rápidamente frente a estos escenarios es cada vez una tarea que demanda más complejidad y por ello; personas y tecnologías.
Desde Datasec evolucionamos en optimizar estos procesos mezclando experiencia, herramientas y tiempo.
La tarea de ciberseguridad sucede en cada instante que se comparte un recurso de información, o cuando la misma tiene un impacto nacional o internacional, y es muy importante tomarse el tiempo y las medidas necesarias para ajustar a los máximos posibles la postura de ciberseguridad. Esto es a través de la limitación de permisos, accesos restringidos y fuertemente autenticados de los administradores, desarrolladores y demás.

Cada día, la inteligencia de amenazas internas y externas genera un profundo estudio y esfuerzo en las organizaciones a diferentes niveles por lo que el apoyo exclusivo y dedicado en las áreas de seguridad de la información de cualquier organización es imprescindible, lo que marcará el futuro de la misma.

¡Sigan protegiéndose!