Boletín de Ciberseguridad

Fecha de Publicación
11/04/2022- N.º 31

Mes de Abril
28/03/2022 -11/04/2022

Datasec

Índice

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 la 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 marzo se destacan 6 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 1 de fraude cibernético y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Zyxel parchea vulnerabilidad crítica que puede permitir secuestros de Firewall y VPN

Zyxel ha emitido parches para una falla de seguridad altamente crítica que brinda a los piratas informáticos maliciosos la capacidad de tomar el control de una amplia gama de firewalls y productos VPN que la empresa vende a otras empresas.

Los piratas informáticos violan datos Mailchimp para lanzar estafas de phishing criptográfico

Mailchimp reveló el lunes una violación de datos que resultó en el compromiso de una herramienta interna para obtener acceso no autorizado a las cuentas de los clientes y realizar ataques de phishing.

Google lanza actualizaciones de seguridad para Chrome

Se han descubierto múltiples vulnerabilidades en el navegador Google Chrome, la más grave de las cuales podría permitir a un atacante aprovechar para tomar el control de un sistema afectado.

spring	**Parches de seguridad para errores críticos en Java Spring Framework**	CRÍTICO

Descripción

Una vulnerabilidad de ejecución remota de código (RCE) de día cero salió a la luz en el marco de Spring.

Estado

Spring Framework lanzó un parche de emergencia para abordar una falla de ejecución remota de código recientemente revelada que, si se explota con éxito, podría permitir que un atacante no autenticado tome el control de un sistema objetivo.

Rastreada como CVE-2022-22965, la falla de alta gravedad afecta las versiones de Spring Framework 5.3.0 a 5.3.17, 5.2.0 a 5.2.19 y otras versiones anteriores no compatibles.

Remediación / Referencias

Se recomienda a los usuarios que actualicen a las versiones 5.3.18 y 5.2.20, o posterior.

Por mayor información acceder a: https://cualesmi-ip.com/blog/vulnerabilidad-de-dia-cero-descubierta-en-java-spring-framework/

QNAP	Vulnerabilidad OpenSSL Infinite Loop afecta a los dispositivos NAS	CRÍTICO

Descripción

QNAP reveló esta semana que un número seleccionado de sus dispositivos de almacenamiento conectado a la red (NAS) se ven afectados por un error recientemente revelado en la biblioteca criptográfica OpenSSL de código abierto.

Estado

Registrado como CVE-2022-0778, el problema se relaciona con un error que surge al analizar los certificados de seguridad para desencadenar una condición de denegación de servicio y bloquear de forma remota los dispositivos sin parchear.

Las versiones afectadas son las siguientes:

- QTS 5.0.x y posterior
- QTS 4.5.4 y posterior
- QTS 4.3.6 y posterior
- QTS 4.3.4 y posterior
- QTS 4.3.3 y posterior
- QTS 4.2.6 y posterior
- QuTS hero h5.0.x y posterior
- QuTS hero h4.5.4 y posterior, y
- QuTScloud c5.0.x

Remediación / Referencias

Se espera que pronto se lancen parches para los sistemas operativos QTS y QuTScloud.

Por mayor información acceder a:
https://diarioinforme.com/qnap-advierte-que-un-error-grave-de-openssl-afecta-a-la-mayoria-de-sus-dispositivos-nas/

ZYXEL	Zyxel parchea vulnerabilidad que puede permitir secuestros de Firewall y VPN	CRÍTICO

Descripción

Zyxel ha emitido parches para una falla de seguridad altamente crítica que brinda a los piratas informáticos maliciosos la capacidad de tomar el control de una amplia gama de firewalls y productos VPN que la empresa vende a las empresas.

Estado

La falla es una vulnerabilidad de omisión de autenticación que se deriva de la falta de un mecanismo de control de acceso adecuado en el CGI (interfaz de puerta de enlace común) de los dispositivos afectados, dijo la compañía. El control de acceso se refiere a un conjunto de políticas que se basan en contraseñas y otras formas de autenticación para garantizar que los recursos o los datos estén disponibles solo para las personas autorizadas. La vulnerabilidad se rastrea como CVE-2022-0342.

Remediación / Referencias

Recomiendan instalar los nuevos firmwares lo antes posible para estar lo más protegidos posible.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/03/vulnerabilidad-lpe-en-windows-que-se.html

mailchimp	**Violación de datos en Mailchimp para lanzar estafas de phishing criptográfico**	PREVENCIÓN

Descripción

Mailchimp reveló el lunes una violación de datos que resultó en el compromiso de una herramienta interna para obtener acceso no autorizado a las cuentas de los clientes y realizar ataques de phishing.

Estado

La compañía se dio cuenta de la intrusión el 26 de marzo después de identificar a un actor malicioso que accedió a una herramienta utilizada por los equipos de atención al cliente y administración de cuentas de la compañía. El acceso se obtuvo luego de un ataque de ingeniería social exitoso, un tipo de ataque que aprovecha el error humano y utiliza técnicas de manipulación para obtener información privada, acceso u objetos de valor.

Aunque Mailchimp declaró que actuó rápidamente, las credenciales desviadas se usaron para acceder a 319 cuentas de MailChimp y exportar más las listas de correo correspondientes a 102 cuentas.

También se cree que el actor no identificado obtuvo acceso a las claves API para un número no especificado de clientes, que según la compañía se deshabilitaron, lo que evita que los

atacantes abusen de las claves API para montar campañas de phishing basadas en correo electrónico.

El reconocimiento se produce cuando la compañía de billeteras de criptomonedas Trezor dijo el domingo que estaba investigando un posible incidente de seguridad derivado de un boletín de suscripción alojado en Mailchimp después de que el actor reutilizó los datos robados para enviar correos electrónicos falsos que afirmaban que la compañía había experimentado un incidente de seguridad.

El correo electrónico fraudulento, que venía con un supuesto enlace para descargar una versión actualizada de Trezor Suite alojada en lo que en realidad es un sitio de phishing, provocó que los destinatarios desprevenidos conectaran sus billeteras, lo que permitió al adversario transferir los fondos a una billetera bajo su control.

Remediación / Referencias

Se recomienda a los clientes que habiliten la autenticación de dos factores para proteger sus cuentas de los ataques de adquisición, y que se abstengan de abrir cualquier correo electrónico de la empresa hasta nuevo aviso.

Para saber más invitamos a visitar el siguiente sitio:
https://blog.segu-info.com.ar/2022/04/robo-de-datos-mailchimp-permite.html

	Apple emite parches para Zero-Day explotados activamente	PREVENCIÓN

Descripción

Apple lanzó el jueves parches de emergencia para abordar dos fallas de día cero en sus sistemas operativos móviles y de escritorio que, según dijo, pueden haber sido explotados en la naturaleza.

Estado

Las deficiencias se han solucionado como parte de las actualizaciones de iOS y iPadOS 15.4.1, macOS Monterey 12.3.1, tvOS 15.4.1 y watchOS 8.5.1. Ambas vulnerabilidades se han informado a Apple de forma anónima.

Rastreado como CVE-2022-22675, el problema se ha descrito como una vulnerabilidad de escritura fuera de los límites en un componente de decodificación de audio y video, llamado AppleAVD que podría permitir que una aplicación ejecute código arbitrario con privilegios de kernel.

Remediación / Referencias

Apple dijo que el defecto se resolvió mejorando la verificación de límites, y agregó que es consciente de que "este problema puede haber sido explotado activamente".

Para saber más invitamos a visitar el siguiente sitio:
https://hackarizona.org/es/apple-emite-parches-para-2-dispositivos-zero-day-explotados-activamente-en-dispositivos-iphone-ipad-y-mac/

Google	**Google lanza actualizaciones de seguridad para Chrome**	PREVENCIÓN

Descripción

Se han descubierto múltiples vulnerabilidades en el navegador Google Chrome, la más grave de las cuales podría permitir a un atacante aprovechar para tomar el control de un sistema afectado.

Estado

Google ha lanzado la versión 100.0.4896.60 de Chrome para Windows, Mac y Linux. Esta versión aborda las vulnerabilidades que un atacante podría aprovechar para controlar una computadora afectada y ver, cambiar o eliminar datos.

Remediación / Referencias

Se recomienda a los usuarios revisar la *Nota de lanzamiento de Chrome* y aplicar la actualización necesaria.

Para saber más invitamos a visitar el siguiente sitio:
https://www.xataka.com/seguridad/usas-chrome-actualiza-cuanto-antes-google-detecta-fallo-seguridad-grave#:~:text=Google%20ha%20lanzado%20una%20actualizaci%C3%B3n,en%20Windows%2C%20Mac%20y%20Linux.

Conclusión

Comenzando la primera quincena de abril, diferentes empresas han optado por realizar procesos de prevención de amenazas y vulnerabilidades en el software.

Los marcos que se actualizan periódicamente nos facilitan el poder entrar en contacto y utilizar las mejores prácticas y conocimientos que han evolucionado rápidamente a través de los cortos períodos de los ciclos de desarrollo de software.

Siempre es recomendable la actualización de todo el software que se encuentra en los sistemas operativos, ya que de esta manera se mitiga el riesgo de exponerse a vulnerabilidades que se puedan encontrar en el software o en los dispositivos.

Los hackers se aprovechan de estas vulnerabilidades a través de un código, para atacar de forma específica, y lo empaquetan en un software malicioso. Esto hace que cualquier equipo pueda ser infectado, sin que el usuario lo perciba, ya sea a través de un sitio web, un email o reproducir soportes infectados.

Una vez que el equipo se encuentra infectado, este software malicioso es capaz de robar datos, permitir que el hacker tome control del equipo e, incluso, utilizar el software con otros fines a los originales.

Cada día, la inteligencia de estas amenazas evoluciona generando una necesidad de estudio y esfuerzo por parte de las organizaciones, por lo que el apoyo exclusivo y dedicado en lasáreas de seguridad de la información de cualquier organización es imprescindible.

Es así, como con nuestras recomendaciones y noticias damos por culminado nuestro informe, como siempre saludando a nuestros lectores.