Boletín de Ciberseguridad

Fecha de Publicación
15/08/2022 - N.º 40
Mes de Agosto
01/08/202 - 15/08/2022

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 primera quincena del mes de agosto 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:

Se eliminaron 10 módulos de PyP

Paquetes maliciosos ingresaron a los repositorios de código abierto y eliminaron 10 módulos del índice de paquetes de Python

Acceden a datos de CISCO

Grupo de ransomware accede a datos de Cisco, no sensibles.

Oracle 349 parches y 64 vulnerabilidades críticas

Oracle anunció que lanzó un total de 349 nuevos parches de seguridad como parte de su Actualización de parches críticos (CPU).

	Se eliminaron 10 módulos de PyP	CRÍTICO

Descripción

Paquetes maliciosos ingresaron a los repositorios de código abierto y eliminaron 10 módulos del índice de paquetes de Python

Estado

Estas bibliotecas fueron eliminadas debido a su capacidad para poder recopilar datos críticos, como contraseñas y tokens de API. Esta lista de paquetes maliciosos fue publicada.
Se han demostrado ser un vector de ataque lucrativo para que los adversarios lleguen a un número significativo de usuarios intermedios disfrazando el malware como bibliotecas aparentemente útiles.

Remediación / Referencias

Se recomienda si se utiliza una de estas bibliotecas de código libre que los creadores de estas se puedan mantener y verificar los paquetes publicados.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/08/bibliotecas-que-roban-datos-en.html
https://www.ciberseguridadlatam.com/2022/08/10/nuevas-bibliotecas-de-python-maliciosas-encontradas-en-el-repositorio-pypi/

	Malware dirigido a usuarios macOS	IMPORTANTE

Descripción

Un malware para espiar dirigido a usuarios de macOS

Estado

Descubrieron un backdoor para macOS previamente desconocido que espía a los usuarios de los equipos Mac comprometidos y que utiliza servicios públicos de almacenamiento en la nube para comunicarse con sus operadores, al cual llamaron Cloud Mensis.
Apple reconoció la presencia de este software espía el cual está dirigido a los usuarios de sus productos, por esta razón ha anunciado el lanzamiento del modo Lockdown para iOS, iPadOS y macOS, esta herramienta desactiva la ejecución del malware.

Remediación / Referencias

Se recomienda actualizar las plataformas macOS.

Por mayor información acceder a:
https://www.welivesecurity.com/la-es/2022/07/20/cloudmensis-malware-espiar-dirigido-usuarios-macos/
https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

CISCO	Acceden a datos de CISCO	CRÍTICO

Descripción

Grupo de ransomware accede a datos de Cisco, no sensibles.

Estado

Se confirmó el ataque a Cisco cuando el grupo de ransomware Yanluowang publicó una lista parcial de los archivos, los cuales fueron robados de Cisco, el grupo de inteligencia confirmó que Cisco, este hecho.

Cisco fue comprometido por primera vez el 24 de mayo, más adelante se convirtió en una violación de red, confirmado por una investigación llevada a cabo por el equipo de Respuestas e Incidentes de seguridad de Cisco (CSIRT). El vector de acceso inicial fue a través del phishing exitoso de la cuenta personal de Google de un empleado, lo que finalmente condujo al compromiso de sus credenciales y acceso a la VPN de Cisco.

Cisco no identificó ningún impacto como resultado de este incidente, incluidos los productos o servicios de Cisco, datos confidenciales de clientes o información confidencial de empleados, propiedad intelectual u operaciones de la cadena de suministro.

Remediación / Referencias

Consejos para prevenir ataques de Phishing, no ingreses a links que no sean seguros, no envíes información personal usando mensajes de correo electrónico y verifique el emisor del correo si es el correcto.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2022/08/grupo-de-ransomware-accede-datos-no.html
https://www.forbes.com/sites/daveywinder/2022/08/13/cisco-hacked-ransomware-gang-claims-it-has-28gb-of-data/?sh=5156c2d34043

Rug Pull: Estafa criptomonedas

IMPORTANTE

Descripción

Rug pull es un modelo de fraude entorno a las criptomonedas.

Estado

Los desarrolladores buscan atraer inversionistas para un nuevo criptoactivo y luego abandonan el proyecto con los fondos recaudados.
Existen tres tipos de Rug Pull, Robo de Liquidez, los desarrolladores incentivan a las víctimas a invertir en sus proyectos para luego escapar con ese dinero; Falsos Invasores, los desarrolladores crean un proyecto con falsos inversores, logrando atraer a las víctimas para invertir en él, luego elevan el precio de las criptomonedas, ganando la confianza de las víctimas para terminar vendiendo todo de forma repentina y bajando los precios de los activos; Manipulación del Proyecto, los desarrolladores impiden la venta de activos a los inversores, sin deber informar previamente. Luego el valor sube y los desarrolladores intercambian todas las monedas y desaparecen.

Remediación / Referencias

Investigar quienes son los creadores del proyecto, tener respaldos, dudar si son demasiado buenas, verificar la fluctuación del valor del criptoactivo.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2022/07/25/que-es-estafa-rug-pull/

Google	Google retrasa el bloqueo de cookies de terceros hasta 2024	PREVENCIÓN

Descripción

Google dijo que cambia sus planes para desactivar las cookies de terceros en el navegador web Chrome desde finales de 2023 hasta la segunda mitad de 2024.

Estado

Google y la tecnología publicitaria dijeron que está adoptando un "enfoque deliberado" y extendiendo la ventana de prueba para sus iniciativas en curso, antes de eliminar gradualmente las cookies de terceros.

Las cookies son piezas de datos que el navegador web coloca en la computadora de un usuario u otro dispositivo cuando se accede a un sitio web, y las cookies de terceros alimentan gran parte del ecosistema de publicidad digital y su capacidad para rastrear a los usuarios en diferentes sitios para mostrar anuncios dirigidos.

Remediación / Referencias

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/07/google-delays-blocking-3rd-party.html

ORACLE	Oracle 349 parches y 64 vulnerabilidades críticas	PREVENCIÓN

Descripción

Oracle anunció que lanzó un total de 349 nuevos parches de seguridad como parte de su Actualización de parches críticos (CPU).

Estado

Fueron incluidos 230 parches para vulnerabilidades que pueden ser explotadas por atacantes remotos no autenticados y para 64 vulnerabilidades de gravedad crítica, incluidas cuatro que tienen una puntuación CVSS de 10.
Oracle anunció que la CPU de 2022 resuelve vulnerabilidades adicionales para muchas aplicaciones. Además, la empresa incluyó parches de terceros para aplicaciones que no recibieron nuevas correcciones de seguridad.

Remediación / Referencias

Se recomienda a los clientes que apliquen las correcciones recién lanzadas lo antes posible, para evitar ser víctimas de intentos de explotación.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2022/07/solo-349-parches-para-oracle-y-64.html

Conclusiones

Esta quincena tuvimos filtraciones masivas de información privada. Esto puede ser utilizado en campañas de ingeniería social dentro de las organizaciones, para reconocer puntos débiles en las personas que trabajan y colaboran.

La responsabilidad, una y otra vez más es de todos y todas; Cuidándonos de llamadas por teléfono, de spam o correos de phishing. Para eso, lo recomendable en estos casos es extremar la precaución con las llamadas o correos que recibamos: Por ejemplo, puede que recibamos correos de hackers haciéndose pasar por LinkedIn, donde sólo buscan que les proporcionemos la contraseña y otra información para poder acceder. Lo recomendable para cerciorarnos si se trata o no de un email real es entrar en la web oficial de LinkedIn y hacer nosotros manualmente los cambios sin pinchar en ningún enlace sospechoso.

¡Y no olviden mantener actualizadas sus plataformas y equipos informáticos!