Boletín de Ciberseguridad N°58

Fecha de publicación: 09/05/2023

Mes de mayo

24/04/2023 – 09/05/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

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 mayo se destacan 6 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Open AI confirma violación de datos de ChatGPT

OpenAI, creador del chatbot ChatGPT impulsado por inteligencia artificial (IA), ha confirmado que un error en el código fuente del chatbot puede haber causado una fuga de datos.

Anuncios de Google para propagar malware

Actores maliciosos están empleando tácticas de SEO y pagando anuncios de Google para engañar a las víctimas, logrando que descarguen malware.

Google presenta un inicio de sesión seguro sin contraseña

El gigante tecnológico comenzó a implementar la solución sin contraseña en las cuentas de Google en todas las plataformas.

Vulnerabilidad Crítica

OpenAI confirma violación de datos de ChatGPT

CRÍTICO

Descripción

OpenAI, creador del chatbot ChatGPT impulsado por inteligencia artificial (IA), ha confirmado que un error en el código fuente del chatbot puede haber causado una fuga de datos.

Estado

Según OpenAI, una vulnerabilidad en la biblioteca de código abierto de Redis utilizada por ChatGPT significaba que "algunos usuarios" podían ver "títulos del historial de chat de otro usuario activo" y potencialmente podían ver el primer mensaje de una nueva conversación, si ambos usuarios estaban activos al mismo tiempo.

La compañía también admitió que el error puede haber causado la "visibilidad involuntaria de la información relacionada con el pago" para los usuarios premium de ChatGPT que estuvieron activos entre la 1 y las 10 a.m. el 20 de marzo. El tipo y los últimos cuatro dígitos del número de tarjeta de pago de los usuarios activos pueden haber sido visibles para otros usuarios durante este período. No se vio la información completa de la tarjeta de pago en ningún momento. OpenAI informó que cree que la cantidad de usuarios afectados por este error es "extremadamente baja".

OpenAI confirmó que, una vez descubierto el error, se parcheó el mismo día. Asimismo, anunció que contactaría a todos los afectados por la fuga de datos.

Luego del incidente, la organización anunció que se asociaría con la plataforma de recompensas por errores Bugcrowd para lanzar un programa de recompensas por errores. El programa es, según OpenAI, parte de su "compromiso con la IA segura" y para "reconocer y recompensar los valiosos conocimientos de los investigadores de seguridad que contribuyen a mantener segura nuestra tecnología y nuestra empresa".

A través del programa de recompensas por errores, las personas podrán informar cualquier falla de seguridad, vulnerabilidad o error que se encuentre en sus sistemas a cambio de una recompensa monetaria. Las recompensas monetarias oscilan entre 200 dólares estadounidenses por hallazgos de "gravedad baja" y 20.000 dólares estadounidenses por "descubrimientos excepcionales".

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/data/news/openai-confirms-chatgpt-data-breach

Anuncios de Google utilizados para propagar malware

CRÍTICO

Descripción

Actores maliciosos están empleando tácticas de SEO y pagando anuncios de Google para engañar a las víctimas, logrando que descarguen malware.

Estado

Se están utilizando anuncios de Google y tácticas de SEO para atraer a las víctimas a hacer clic en enlaces envenenados con malware.

Según investigadores, los actores maliciosos han estado utilizando instaladores de anuncios envenenados como troyanos, específicamente para propagar el malware Bumblebee. Estos instaladores de anuncios están asociados con varias empresas conocidas, como Zoom, Citrix Workspace, Cisco AnyConnect y ChatGPT de OpenAI. Se descubrió que un actor malintencionado no solo había creado un instalador de anuncios envenenado para Cisco AnyConnect, sino también una página de descarga falsa para el malware. Pudieron hacer esto explotando un sitio de WordPress comprometido.

Una vez que descargado el malware Bumblebee, los actores maliciosos lo utilizan con mayor frecuencia para lanzar ransomware dentro del dispositivo infectado. En uno de los casos investigados, se descubrió que el actor malintencionado se movía lateralmente por el dispositivo, descargando y ejecutando una serie de aplicaciones y programas de software, incluidas las herramientas legítimas de acceso remoto AnyDesk y Dameware, así como el malware de pruebas de penetración Cobalt Strike.

Mediante el uso de anuncios de pago de Google, así como tácticas de SEO en sus páginas de descarga falsas, los atacantes pueden asegurarse de que sus cargas troyanizadas y envenenadas estén en la parte superior de la página de resultados de búsqueda de Google, lo que significa que es más probable que las víctimas hagan clic en ellas.

Remediación / Referencias

Para evitar ser víctima de anuncios envenenados, solo descargue software y actualizaciones de sitios confiables y vaya a los sitios directamente para evitar hacer clic en un enlace troyano.

Por mayor información acceder a:

https://www.cshub.com/malware/news/google-ads-are-being-used-to-spread-malware

CISA: RCE crítico afecta unidades terminales remotas

CRÍTICO

Descripción

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) publicó un aviso de Sistemas de Control Industrial (ICS) sobre una falla crítica que afecta a las unidades terminales remotas ME RTU.

Estado

La vulnerabilidad de seguridad recibió la calificación de gravedad más alta de 10.0 en el sistema de puntuación CVSS por su baja complejidad de ataque.

"La explotación exitosa de esta vulnerabilidad podría permitir la ejecución remota de código", informó CISA, describiéndolo como un caso de inyección de comando que afecta a las versiones del firmware INEA ME RTU anteriores a la versión 3.36.

CISA también publicó una alerta relacionada con varios agujeros de seguridad conocidos en los procesadores Intel(R) que afectan a los productos de automatización de fábrica (FA) de Mitsubishi Electric y que podrían resultar en una escalada de privilegios y una condición de denegación de servicio (DoS).

El desarrollo se produce cuando la agencia recomendó a las organizaciones de infraestructura crítica que tomen las medidas necesarias para asegurar las cadenas de suministro mediante la revisión de la Lista cubierta de la Comisión Federal de Comunicaciones (FCC) de equipos de comunicaciones que se consideran un riesgo para la seguridad nacional.

CISA también ha instado a las entidades a adoptar la guía emitida por NIST para identificar, evaluar y mitigar los riesgos de la cadena de suministro, e inscribirse en el servicio gratuito de Escaneo de Vulnerabilidad de la agencia para identificar dispositivos vulnerables y de alto riesgo.

Además, siguen los esfuerzos realizados por las autoridades de ciberseguridad en Australia, Canadá, el Reino Unido, Alemania, los Países Bajos, Nueva Zelanda y los EE. UU. para "tomar las medidas urgentes necesarias para enviar productos que son seguros por diseño y por defecto".

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/05/cisa-issues-advisory-on-critical-rce.html

	Explotación activa de vulnerabilidades de TP-Link, Apache y Oracle detectadas	CRÍTICO

Descripción

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha agregado tres fallas al catálogo de Vulnerabilidades Explotadas Conocidas (KEV), según evidencia de explotación activa.

Estado

Las vulnerabilidades de seguridad son las siguientes:

- Vulnerabilidad de inyección de comando TP-Link Archer AX-21, con un puntaje CVSS: 8.8.

  Refiere a un caso de inyección de comandos que afecta a los enrutadores **TP-Link Archer AX-21** que podrían explotarse para lograr la ejecución remota de código. Según investigadores de seguridad, los actores de amenazas asociados con la botnet Mirai han utilizado la falla desde el 11 de abril de 2023.

- Vulnerabilidad de deserialización de Apache Log4j2 de datos no confiables, con un puntaje CVSS: 9,0.

  Se trata de una ejecución remota de código que afecta la biblioteca de registro Apache Log4j2 que salió a la luz en diciembre de 2021. Actualmente no está claro cómo se abusa de esta vulnerabilidad específica, aunque los datos recopilados muestran evidencia de intentos de explotación de hasta 74 direcciones IP únicas en los últimos 30 días.

- Vulnerabilidad no especificada del servidor Oracle WebLogic, con un puntaje CVSS: 7,5.

  Un error de alta gravedad en Oracle WebLogic Server versiones 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0 que podría permitir el acceso no autorizado a datos confidenciales. Fue parcheado por la compañía como parte de las actualizaciones lanzadas en enero de 2023.

  Oracle WebLogic Server contiene una vulnerabilidad no especificada que permite que un atacante no autenticado con acceso a la red a través de T3, IIOP, comprometa Oracle WebLogic Server.

  Si bien existen explotaciones de prueba de concepto (PoC) para la falla, no parece haber ningún informe público de explotación maliciosa.

Remediación / Referencias

Se deben aplicar las correcciones proporcionadas por los proveedores antes del 22 de mayo de 2023 para proteger sus redes contra estas amenazas activas.

Por mayor información acceder a:

https://thehackernews.com/2023/05/active-exploitation-of-tp-link-apache.html

Prevención

Google presenta un inicio de sesión seguro sin contraseñas

PREVENCIÓN

Descripción

El gigante tecnológico comenzó a implementar la solución sin contraseña en las cuentas de Google en todas las plataformas.

Estado

Las claves de acceso, respaldadas por FIDO Alliance, son una forma más segura de iniciar sesión en aplicaciones y sitios web sin tener que usar una contraseña tradicional. Esto, a su vez, se puede lograr simplemente desbloqueando su computadora o dispositivo móvil con sus datos biométricos (por ejemplo, huella digital o reconocimiento facial) o un PIN local.

“Y, a diferencia de las contraseñas, las claves de paso son resistentes a los ataques en línea como el phishing, lo que las hace más seguras que cosas como los códigos SMS de un solo uso", informó Google.

Las claves de acceso, una vez creadas, se almacenan localmente en el dispositivo y no se comparten con ninguna otra parte. Esto también elimina la necesidad de configurar la autenticación de dos factores, ya que demuestra que tiene acceso a su dispositivo y puede desbloquearlo.

Los usuarios también tienen la opción de crear claves de acceso para cada dispositivo que utilicen para iniciar sesión en la cuenta de Google. Dicho esto, una clave de paso creada en el iPhone estará disponible en otros dispositivos si han iniciado sesión en la misma cuenta de iCloud.

Vale la pena señalar que tanto el Administrador de contraseñas de Google como el llavero de iCloud usan cifrado de extremo a extremo para mantener la privacidad de las claves de acceso, lo que evita que los usuarios queden bloqueados en caso de que pierdan el acceso a sus dispositivos o facilitan la actualización de un dispositivo a otro.

Además, los usuarios pueden iniciar sesión en un nuevo dispositivo o usar temporalmente un dispositivo diferente seleccionando la opción "usar una clave de paso de otro dispositivo", que luego usa el bloqueo de pantalla y la proximidad del teléfono para aprobar un inicio de sesión único.

“Luego, el dispositivo verifica que su teléfono está cerca mediante un pequeño mensaje anónimo de Bluetooth y establece una conexión cifrada de extremo a extremo con el teléfono a través de Internet", explicó la compañía.

El teléfono usa esta conexión para entregar su firma de clave de acceso única, que requiere su aprobación y el paso biométrico o de bloqueo de pantalla en el teléfono. Ni la clave de acceso en sí ni la información de bloqueo de pantalla se envían al nuevo dispositivo.

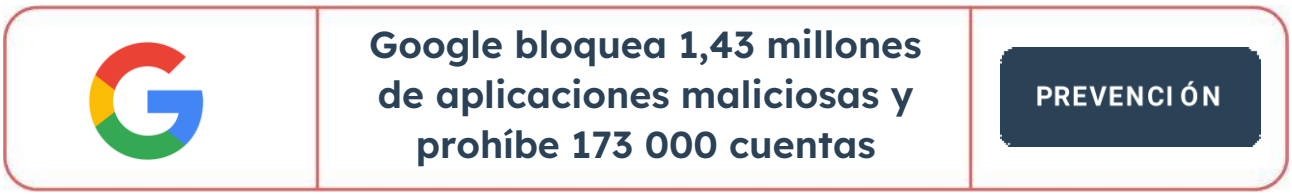
Si bien este puede ser el "comienzo del fin de la contraseña", la compañía dijo que tiene la intención de continuar admitiendo los métodos de inicio de sesión existentes, como contraseñas y autenticación de dos factores, en el futuro previsible.

Remediación / Referencias

Google recomienda que los usuarios no creen claves de acceso en dispositivos que se comparten con otros, una medida que podría socavar todas sus protecciones de seguridad.

Por mayor información acceder a:

https://thehackernews.com/2023/05/google-introduces-passwordless-secure.html



Descripción

Google reveló que sus funciones de seguridad mejoradas y los procesos de revisión de aplicaciones lo ayudaron a bloquear la publicación de 1,43 millones de aplicaciones maliciosas en Play Store en 2022.

Estado

La compañía también prohibió 173,000 cuentas maliciosas y evitó más de USD $2 mil millones en transacciones fraudulentas y abusivas a través de funciones para desarrolladores como API de compras anuladas, ID de cuenta ofuscada y API de integridad de juegos.

La adición de métodos de verificación de identidad como número de teléfono y dirección de correo electrónico para unirse a Google Play contribuyó a una reducción en las cuentas utilizadas para publicar aplicaciones que van en contra de sus políticas, señaló Google.

El gigante de las búsquedas dijo además que "evitó que alrededor de 500.000 aplicaciones enviadas accedieran innecesariamente a permisos confidenciales en los últimos 3 años".

El desarrollo se produce semanas después de que Google promulgara una nueva política de eliminación de datos que requiere que los desarrolladores de aplicaciones ofrezcan una "opción fácilmente detectable" a los usuarios tanto dentro como fuera de una aplicación.

A pesar de estos esfuerzos de Google, los ciberdelincuentes continúan encontrando formas de eludir las protecciones de seguridad de la tienda de aplicaciones y publican aplicaciones maliciosas y de adware.

Remediación / Referencias

Google recomienda descargar aplicaciones de fuentes confiables, limítese a descargar aplicaciones de Google Play Store, que es la tienda de aplicaciones oficial para dispositivos Android. Evite descargar aplicaciones de sitios web o tiendas de aplicaciones de terceros, ya que es más probable que alojen aplicaciones maliciosas.

Por mayor información acceder a:

https://thehackernews.com/2023/05/google-blocks-143-million-malicious.html

Conclusiones

En el mundo digital actual, la ciberseguridad se ha vuelto más importante que nunca.

Una de las mayores amenazas para la ciberseguridad es la prevalencia de aplicaciones maliciosas. Para mantenerse seguro, es importante descargar aplicaciones únicamente de fuentes confiables, como las tiendas de aplicaciones oficiales. También es importante leer detenidamente los permisos de las aplicaciones antes de instalar una aplicación y otorgar sólo los permisos necesarios para la funcionalidad de la aplicación. Además, la instalación de una aplicación antivirus confiable puede proporcionar una capa adicional de protección contra el malware y otras amenazas de seguridad.

Otros pasos importantes para mantenerse seguro incluyen mantener su dispositivo y aplicaciones actualizados con los últimos parches de seguridad y ser cauteloso al hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas. Al seguir estas recomendaciones, puede ayudar a protegerse de las amenazas de ciberseguridad y disfrutar de una experiencia en línea más segura.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Sigan protegiéndose!