Boletín de Ciberseguridad N°63

Fecha de publicación: 26/07/2023

Mes de julio

10/06/2023 – 26/07/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Vulnerabilidad Crítica
Datos de Estee Lauder robados en ciberataque.....5
Filtración de datos de Roblox expone datos de empleados.....7
Zero day crítico en los instaladores de Windows Atera.....8
Vulnerabilidad de OpenSSH expone los sistemas Linux a la inyección de comandos remotos.....9
Error de Microsoft permitió la utilización de tokens Azure AD falsificados.....12
Fuga de datos de VirusTotal expone los detalles de algunos clientes registrados.....13
Conclusiones.....15

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 julio se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

Datos de Estee Lauder robados en ciberataque

Ciberdelincuentes se infiltraron en los sistemas de la empresa e interrumpieron sus procesos comerciales.

Filtración de datos de Roblox expone datos de empleados

Es posible que a los desarrolladores que asistieron a la conferencia de desarrolladores de Roblox les hayan robado sus datos.

Vulnerabilidad de OpenSSH expone los sistemas Linux a la inyección de comandos remotos

Surgen detalles sobre una falla ahora parcheada en OpenSSH que podría explotarse potencialmente para ejecutar comandos arbitrarios de forma remota en hosts

comprometidos bajo condiciones específicas.

Vulnerabilidad Crítica

ESTĒE LAUDER	Datos de Estee Lauder robados en ciberataque	CRÍTICO

Descripción

Ciberdelincuentes se infiltraron en los sistemas de la empresa e interrumpieron sus procesos comerciales.

Estado

La empresa de cosméticos Estee Lauder sufrió recientemente un ciberataque que interrumpió sus procesos comerciales.

Un actor malicioso logró robar datos de los sistemas de la empresa y causar interrupciones en el proceso. Estee Lauder no ha hecho público cómo el hacker pudo infiltrarse en sus sistemas.

En un comunicado sobre el incidente, la compañía de cosméticos informó que estaba trabajando para proteger y restaurar los sistemas afectados por el ataque cibernético. Esto incluyó la eliminación de algunos de los sistemas afectados.

Estee Lauder anunció el inicio de una investigación sobre la violación de datos para comprender qué y cuánto robaron los piratas informáticos durante el ataque cibernético. La compañía también informó que se ha puesto en contacto con expertos en seguridad cibernética y policiales con respecto al ataque.

Varias empresas estadounidenses han sufrido ciberataques en los últimos seis meses, incluidas Nickelodeon, Blizzard Entertainment, Reddit y Yum!.

Ataque de ransomware contra Yum!

Corporación estadounidense de comida rápida Yum! Brands, propietaria de franquicias como KFC, Pizza Hut y Taco Bell, sufrió una violación de datos luego de un ataque de ransomware.

Yum! Brands sufrió un ataque de similares características durante el mes de Enero, éste involucró a un actor malicioso que obtuvo acceso no autorizado a Yum!, mediante un ataque de ransomware interrumpió los procesos comerciales de la empresa y cerró sus sistemas de TI, lo que provocó que aproximadamente 300 restaurantes en todo el Reino Unido estuvieran temporalmente cerrados.

Yum! informó que "tomó medidas para bloquear los sistemas afectados, notificó a las autoridades federales encargadas de hacer cumplir la ley, trabajó con los principales equipos forenses digitales y de restauración para investigar y recuperarse del incidente e implementó una tecnología mejorada de detección y monitoreo las 24 horas del día, los 7 días de la semana".

Después del ataque cibernético, se inició una investigación sobre el ataque para ver si se habían robado datos durante el mismo. La investigación mostró que se había accedido a datos privados de los empleados durante el incidente.

Estos datos robados incluían los nombres y números de tarjetas de identificación de algunos empleados, incluidos los números de licencia de conducir. En u

n aviso del incumplimiento enviado a los afectados, Yum! dijo que “no había evidencia de robo de identidad o fraude” cometido con los datos robados.

La organización declaró que "no espera que este evento tenga un impacto adverso significativo en su negocio, operaciones o resultados financieros" en un informe presentado ante la Comisión de Bolsa y Valores de EE. UU. con respecto al ataque.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/iotw-estee-lauder-data-stolen-in-cyber-attack

ROBLOX	**Filtración de datos de Roblox expone datos de empleados**	CRÍTICO

Descripción

Es posible que a los desarrolladores que asistieron a la conferencia de desarrolladores de Roblox les hayan robado sus datos.

Estado

Es posible que se hayan filtrado los datos personales de los asistentes a la Conferencia de desarrolladores de Roblox entre 2017 y 2021.

El creador del sitio Have I Been Pwned, dió a conocer la noticia de la violación de datos en X (anteriormente conocido como Twitter). Have I Been Pwned permite a los usuarios buscar su nombre y detalles para ver si se han filtrado en alguna violación de datos.

En un mensaje anónimo enviado al creador del sitio, una fuente informó sobre una filtración de datos de todos los participantes de la Conferencia de desarrolladores de Roblox. Según la fuente, los datos a los que se accedió durante el ataque cibernético incluían nombres completos, fechas de nacimiento, correo electrónico, direcciones de casa e IP y números de teléfono. La fuente también informó que estos datos ya se encontraban publicados en línea.

La filtración se volvió a publicar en línea recientemente, donde había atraído una "atención significativa" de partes maliciosas y no maliciosas. Esta nueva publicación de datos robados había visto a "usuarios de alto perfil" recibir "llamadas, mensajes de texto y correos electrónicos maliciosos".

El 20 de julio, Roblox abordó la fuga de datos y se puso en contacto con todos los afectados para resarcir el daño.

Con respecto a las notificaciones de fuga de datos, Roblox dijo que: "Los usuarios mínimamente afectados acaban de recibir un correo electrónico de disculpa. Para los usuarios más gravemente afectados, obtuvieron un año de protección de identidad y una disculpa para todos los demás".

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/roblox-data-breach-exposes-employee-data

Descripción

Las vulnerabilidades de día cero en los instaladores de Windows para el software de administración y monitoreo remoto Atera podrían actuar como un trampolín para lanzar ataques de escalada de privilegios.

Estado

Las fallas se solucionaron en las versiones 1.8.3.7 y 1.8.4.9 lanzadas por Atera el 17 de abril de 2023 y el 26 de junio de 2023, respectivamente.

Investigadores de seguridad, informaron que la capacidad de iniciar una operación desde un contexto NT AUTHORITY\SYSTEM puede presentar riesgos potenciales de seguridad si no se gestiona adecuadamente. Por ejemplo, los atacantes pueden aprovechar las acciones personalizadas mal configuradas que se ejecutan como NT AUTHORITY\SYSTEM para ejecutar ataques de escalada de privilegios locales.

La explotación exitosa de tales debilidades podría allanar el camino para la ejecución de código arbitrario con privilegios elevados.

Ambos defectos residen en la funcionalidad de reparación del instalador MSI, lo que podría crear un escenario en el que las operaciones se activan desde un contexto NT AUTHORITY\SYSTEM incluso si las inicia un usuario estándar.

Según la firma de inteligencia de amenazas propiedad de Google, Atera Agent es susceptible a un ataque de escalada de privilegios local que puede explotarse mediante el secuestro de DLL que luego podría abusarse para obtener un Símbolo del sistema como usuario NT AUTHORITY\SYSTEM.

La segunda falla, por otro lado, se refiere a la "ejecución de comandos del sistema que activan Windows Console Host (conhost.exe) como un proceso secundario", como resultado, se abre una "ventana de comandos que, si se ejecuta con privilegios elevados, puede ser explotada por un atacante para realizar un ataque de escalada de privilegios local".

Las acciones personalizadas mal configuradas pueden ser triviales de identificar y explotar, por lo que presentan riesgos de seguridad significativos para las organizaciones. Es esencial que los desarrolladores de software revisen minuciosamente sus acciones personalizadas para evitar que los atacantes secuestren las operaciones de NT AUTHORITY\SYSTEM desencadenadas por las reparaciones de MSI.

La divulgación se produce cuando Kaspersky arrojó más luz sobre una grave falla de escalamiento de privilegios ahora corregida en Windows (con un puntaje CVSS: 9.8) que ha sido objeto de explotación activa en la naturaleza por parte de los actores de amenazas que utilizan una tarea, mensaje o evento de calendario de Outlook especialmente diseñado.

Si bien Microsoft reveló anteriormente que desde Rusia armaron el error en abril de 2022, la evidencia recopilada por el proveedor de antivirus reveló que un atacante desconocido llevó a cabo intentos de explotación en el mundo real dirigidos a entidades gubernamentales y de infraestructura crítica en Jordania, Polonia, Rumania, Turquía y Ucrania un mes antes de la divulgación pública.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/critical-zero-days-in-atera-windows.html

SSH	**Vulnerabilidad de OpenSSH expone los sistemas Linux a la inyección de comandos remotos**	CRÍTICO

Descripción

Surgen detalles sobre una falla ahora parcheada en OpenSSH que podría explotarse potencialmente para ejecutar comandos arbitrarios de forma remota en hosts comprometidos bajo condiciones específicas.

Estado

Esta vulnerabilidad permite que un atacante remoto ejecute potencialmente comandos arbitrarios en el ssh-agent reenviado de OpenSSH vulnerable.

La vulnerabilidad afecta a todas las versiones de OpenSSH anteriores a la 9.3p2.

OpenSSH es una herramienta de conectividad popular para el inicio de sesión remoto con el protocolo SSH que se utiliza para cifrar todo el tráfico para eliminar las escuchas ilegales, el secuestro de conexiones y otros ataques.

La explotación exitosa requiere la presencia de ciertas bibliotecas en el sistema de la víctima y que el agente de autenticación SSH se reenvíe a un sistema controlado por el atacante. El agente SSH es un programa en segundo plano que mantiene las claves de los usuarios en la memoria y facilita los inicios de sesión remotos en un servidor sin tener que ingresar su frase de contraseña nuevamente.

Investigadores informaron que mientras se examinaba el código fuente de ssh-agent, notaron que un atacante remoto, que tiene acceso al servidor remoto donde se reenvía el ssh-agent de Alice, puede cargar (dlopen()) e inmediatamente descargar (dlclose()) cualquier biblioteca compartida en /usr/lib* en la estación de trabajo de Alice (a través de su ssh-agent reenviado, si está compilado con ENABLE_PKCS11, que es el valor predeterminado).

A través de una empresa de seguridad fué posible diseñar una prueba de concepto (PoC) exitosa contra las instalaciones predeterminadas de Ubuntu Desktop 22.04 y 21.10, aunque se espera que otras distribuciones de Linux también sean vulnerables.

Se recomienda encarecidamente que los usuarios de OpenSSH actualicen a la versión más reciente para protegerse contra posibles amenazas cibernéticas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/new-openssh-vulnerability-exposes-linux.html

Microsoft	**Error de Microsoft permitió la utilización de tokens Azure AD falsificados**	PREVENCIÓN

Descripción

Microsoft anunció que está expandiendo las capacidades de registro en la nube para ayudar a las organizaciones a investigar incidentes de seguridad cibernética y obtener más visibilidad después de enfrentar críticas a raíz de una reciente campaña de ataque de espionaje dirigida a su infraestructura de correo electrónico.

Estado

El gigante tecnológico informó que está haciendo el cambio en respuesta directa a la creciente frecuencia y evolución de las amenazas cibernéticas de los estados nacionales. Se espera que se implemente a partir de septiembre de 2023 para todos los clientes gubernamentales y comerciales.

“En los próximos meses, incluiremos acceso a registros de seguridad en la nube más amplios para nuestros clientes de todo el mundo sin costo adicional”, dijo Microsoft. "A medida que estos cambios surtan efecto, los clientes pueden usar Microsoft Purview Audit para visualizar de forma centralizada más tipos de datos de registro en la nube generados en toda su empresa".

Como parte de este cambio, se espera que los usuarios reciban acceso a registros detallados de acceso al correo electrónico y más de otros 30 tipos de datos de registro que anteriormente solo estaban disponibles en el nivel de suscripción de Microsoft Purview Audit (Premium). Además de eso, el fabricante de Windows dijo que está extendiendo el período de retención predeterminado para los clientes de Audit Standard de 90 días a 180 días.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA, por sus siglas en inglés) acogió con beneplácito la medida y afirmó que "tener acceso a datos de registro clave es importante para mitigar rápidamente las intrusiones cibernéticas" y que es "un paso significativo hacia el avance de los principios de seguridad por diseño".

El desarrollo se produce después de las revelaciones de que un actor de amenazas que opera desde China, denominado Storm-0558, se infiltró en 25 organizaciones al explotar un error de validación en el entorno de Microsoft Exchange.

El Departamento de Estado de EE. UU., que fue una de las entidades afectadas, dijo que pudo detectar la actividad maliciosa de los buzones en junio de 2023 debido al registro mejorado en Microsoft Purview Audit, específicamente usando la acción de auditoría de buzones MailItemsAccessed, lo que llevó a Microsoft a investigar el incidente.

Pero otras organizaciones afectadas dijeron que no pudieron detectar que fueron violadas porque no eran suscriptores de las licencias E5/A5/G5, que vienen con acceso elevado a varios tipos de registros que serían cruciales para investigar el ataque.

Mientras tanto, Microsoft continúa investigando las intrusiones, pero hasta la fecha la compañía no ha explicado cómo los piratas informáticos pudieron adquirir una clave de firma de consumidor de cuenta de Microsoft (MSA) inactiva para falsificar tokens de autenticación y obtener acceso ilícito a cuentas de correo electrónico de clientes usando Outlook Web Access en Exchange Online (OWA) y Outlook.com.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/microsoft-expands-cloud-logging-to.html

Descripción

Los datos asociados con un subconjunto de clientes registrados de VirusTotal, incluidos sus nombres y direcciones de correo electrónico, quedaron expuestos después de que un empleado subiera inadvertidamente la información a la plataforma de análisis de malware.

Estado

El incidente de seguridad, que comprende una base de datos de 5600 nombres en un archivo de 313 KB.

Lanzado en 2004, VirusTotal es un servicio popular que analiza archivos y URL sospechosos para detectar tipos de malware y contenido malicioso mediante motores antivirus y escáneres de sitios web. Fue adquirida por Google en 2012 y se convirtió en subsidiaria de la unidad Chronicle de Google Cloud en 2018.

Google confirmó la filtración e informó que medidas inmediatas fueron tomadas para eliminar los datos.

"Somos conscientes de la distribución no intencional de un pequeño segmento de correos electrónicos de administradores de grupos de clientes y nombres de organizaciones por parte de uno de nuestros empleados en la plataforma VirusTotal", dijo el portavoz de Google Cloud.

"Eliminamos la lista de la plataforma una hora después de su publicación y estamos analizando nuestros procesos internos y controles técnicos para mejorar nuestras operaciones en el futuro".

Entre los datos se incluyen cuentas vinculadas a organismos oficiales de EE. UU., como el Comando Cibernético, el Departamento de Justicia, la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad Nacional (NSA). Otras cuentas pertenecen a agencias gubernamentales en Alemania, los Países Bajos, Taiwán y el Reino Unido.

El año pasado, la Oficina Federal de Seguridad de la Información (BSI) de Alemania advirtió contra la carga automática de archivos adjuntos de correo electrónico sospechosos a VirusTotal, y señaló que hacerlo podría conducir a la exposición de información confidencial.

VirusTotal se disculpó el viernes por el reciente incidente de exposición de datos de clientes, afirmando que fue causado por un empleado que subió accidentalmente un archivo CSV a la plataforma, que contenía información relacionada con sus clientes de cuentas Premium, en particular sus nombres, nombres de grupos asociados de VirusTotal y las direcciones de correo electrónico de los administradores del grupo.

La subsidiaria de Google Chronicle dijo que el archivo solo era accesible para sus socios y clientes corporativos, y que fue el resultado de un error humano y no un ataque cibernético o una vulnerabilidad en sus sistemas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/07/virustotal-data-leak-exposes-some.html

Conclusiones

La situación de la ciberseguridad en el mundo actualmente se enfrenta a desafíos significativos debido al creciente número de actores maliciosos y amenazas cibernéticas. Con el avance tecnológico y la interconexión global, las vulnerabilidades en sistemas, redes y dispositivos se han convertido en un blanco atractivo para individuos y grupos con intenciones dañinas. Estos actores maliciosos pueden variar desde hackers individuales hasta cibergrupos patrocinados por estados o ciberdelincuentes organizados.

La conciencia y la educación en materia de ciberseguridad son esenciales para protegerse tanto a nivel personal como empresarial. Las buenas prácticas de seguridad, como el uso de contraseñas fuertes, la autenticación de dos factores, el cifrado de datos y la actualización regular de software, son fundamentales para mantener la integridad de nuestros sistemas y dispositivos.

Además, las organizaciones y gobiernos deben colaborar y compartir información sobre las amenazas cibernéticas para fortalecer la defensa colectiva contra estos actores maliciosos. La cooperación internacional es crucial, ya que muchas amenazas cibernéticas trascienden fronteras y requieren una respuesta coordinada a nivel global.

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

¡Hasta la próxima!