Boletín de Ciberseguridad N°67

Fecha de publicación: 29/09/2023

Mes de setiembre

11/09/2023 – 29/09/2023

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 segunda quincena del mes de setiembre se destacan 6 noticias de relevancia, siendo 5 de estas sobre vulnerabilidades tecnológicas y 1 sobre prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Ransomware roba 6.8 TB de datos de Save The Children

A la organización benéfica le robaron datos financieros, médicos y de salud en el ciberataque.

Defectos de alta gravedad en Atlassian y en el servidor ISC BIND

Atlassian e Internet Systems Consortium (ISC) han revelado varias fallas de seguridad que afectan a sus productos y que podrían explotarse para lograr denegación de servicio (DoS) y ejecución remota de código.

Duolingo: 2,6 millones de datos publicados en la dark web

Los datos fueron extraídos usando una interfaz abierta de planificación de aplicaciones (API).

Vulnerabilidad Crítica

Save the Children	Ransomware roba 6.8 TB de datos de Save The Children	CRÍTICO

Descripción

A la organización benéfica le robaron datos financieros, médicos y de salud en el ciberataque.

Estado

La banda de ransomware BianLian se ha atribuido la responsabilidad de un ciberataque contra la organización sin fines de lucro Save The Children International.

La banda de ransomware ha estado activa desde junio de 2022 y se dirige principalmente a infraestructuras críticas y organizaciones de atención médica. En ataques anteriores, BianLian extorsionó a estas organizaciones para obtener sus datos.

Si bien la organización benéfica no fue nombrada directamente por la banda de ransomware, en una publicación en su sitio de filtración de datos en la dark web, BianLian identificó a la organización benéfica como "la organización sin fines de lucro líder en el mundo" y dijo que dicha organización sin fines de lucro genera 2.800 millones de dólares en ingresos y opera en 116 países. Esta información ha llevado a sugerir que Save The Children era la organización sin fines de lucro objetivo del ciberataque. La propia organización benéfica confirmó más tarde que había sido víctima de una violación de datos en un comunicado al sitio de noticias The Register.

Según la banda de ransomware, pudo robar más de 6,8 TB de datos de la organización benéfica, que incluyen una amplia gama de datos personales y comerciales. Los presuntos datos robados incluyen 800 GB de registros financieros, así como mensajes de correo electrónico, archivos internacionales de recursos humanos y datos personales, incluidos datos médicos y de salud.

Con respecto al incidente de seguridad cibernética, un portavoz de Save The Children informó a The Register: “Save the Children International experimentó recientemente un incidente de TI que implicó el acceso no autorizado a parte de nuestra red. No ha habido ninguna interrupción operativa y la organización continúa funcionando con normalidad para construir un futuro mejor para los niños de todo el mundo. Estamos trabajando arduamente con especialistas externos para comprender qué sucedió y qué datos se vieron afectados para que podamos tomar todos los pasos apropiados. Este proceso es complejo y lleva tiempo, pero sigue siendo nuestra prioridad absoluta”.

La organización benéfica dijo que había asegurado sus sistemas luego de la violación de datos y que "confía en la integridad continua de nuestra infraestructura de TI".

La empresa destacó que, si bien los incidentes de seguridad cibernética son "una realidad que enfrentan todas las organizaciones", la organización benéfica está decepcionada de que "Save the Children, cuyo objetivo principal es ayudar a los más necesitados, también esté sujeto a tal actividad injustificada".

Se está llevando a cabo una investigación sobre el ciberataque y Save The Children ha prometido que trabajará con las autoridades pertinentes y llegará al fondo de esto. La organización sin fines de lucro agradeció a todo su personal y seguidores por su paciencia y comprensión tras el ciberataque.

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/attacks/news/ransomware-gang-steals-68tb-of-data-from-save-the-children

Microsoft	Microsoft se exponen accidentalmente 38 terabytes de datos confidenciales	CRÍTICO

Descripción

Microsoft informa que se tomaron medidas para corregir un flagrante error de seguridad que llevó a la exposición de 38 terabytes de datos privados.

Estado

La filtración se descubrió en el repositorio de IA GitHub de la compañía y se hizo pública sin darse cuenta al publicar un conjunto de datos de entrenamiento de código abierto. También incluía una copia de seguridad en disco de las estaciones de trabajo de dos ex empleados que contenían secretos, claves, contraseñas y más de 30.000 mensajes internos de Teams.

Ya no se puede acceder al repositorio, denominado "robust-models-transfer". Antes de su eliminación, presentaba código fuente y modelos de aprendizaje automático pertenecientes a un artículo de investigación de 2020 titulado "¿Los modelos ImageNet adversariamente robustos se transfieren mejor?"

La exposición se produjo como resultado de un token SAS demasiado permisivo, una característica de Azure que permite a los usuarios compartir datos de una manera que es difícil de rastrear y de revocar.

Específicamente, el archivo README.md del repositorio indicaba a los desarrolladores que descargaran los modelos desde una URL de Azure Storage que accidentalmente también otorgaba acceso a toda la cuenta de almacenamiento, exponiendo así datos privados adicionales.

Además del alcance de acceso demasiado permisivo, el token también estaba mal configurado para permitir permisos de "control total" en lugar de "solo lectura". Es decir, un atacante no sólo podría ver todos los archivos en la cuenta de almacenamiento, sino que también podría eliminar y sobrescribir los archivos existentes.

En respuesta a los hallazgos, Microsoft dijo que su investigación no encontró evidencia de exposición no autorizada de datos de clientes y que "ningún otro servicio interno fue puesto en riesgo debido a este problema". También enfatizó que los clientes no necesitan realizar ninguna acción por su parte.

Los fabricantes de Windows señalaron además que revocaron el token SAS y bloquearon todo acceso externo a la cuenta de almacenamiento. El problema se resolvió dos días después de la divulgación responsable.

Para mitigar dichos riesgos en el futuro, la compañía ha ampliado su servicio de escaneo secreto para incluir cualquier token SAS que pueda tener vencimientos o privilegios demasiado permisivos. Dijo que también identificó un error en su sistema de escaneo que marcó la URL SAS específica en el repositorio como un falso positivo.

Debido a la falta de seguridad y gobernanza de los tokens Account SAS, deben considerarse tan sensibles como la propia clave de la cuenta. Por lo tanto, se recomienda encarecidamente evitar el uso de Account SAS para compartir externamente. Los errores en la creación de tokens pueden pasar desapercibidos fácilmente y exponer datos confidenciales.

Esta no es la primera vez que salen a la luz cuentas de almacenamiento de Azure mal configuradas. En julio de 2022, investigadores destacaron un escenario en el que un actor de amenazas podría aprovechar dichas cuentas para obtener acceso a un entorno empresarial local.

El desarrollo es el último error de seguridad en Microsoft y se produce casi dos semanas después de que la compañía revelara que piratas informáticos con sede en China pudieron infiltrarse en los sistemas de la compañía y robar una clave de firma altamente sensible al comprometer la cuenta corporativa de un ingeniero y probablemente acceder a un volcado de seguridad del sistema de firma del consumidor.

La IA abre un enorme potencial para las empresas de tecnología. Sin embargo, a medida que los científicos e ingenieros de datos se apresuran para llevar a producción nuevas soluciones de IA, las enormes cantidades de datos que manejan requieren controles y salvaguardias de seguridad adicionales.

Esta tecnología emergente requiere grandes conjuntos de datos para entrenar. Dado que muchos equipos de desarrollo necesitan manipular cantidades masivas de datos,

compartirlos con sus pares o colaborar en proyectos públicos de código abierto, casos como el de Microsoft son cada vez más difíciles de monitorear y evitar.

Remediación / Referencias

Por mayor información acceder a: https://thehackernews.com/2023/09/microsoft-ai-researchers-accidentally.html

Defectos de alta gravedad en Atlassian y en el servidor ISC BIND

CRÍTICO

Descripción

Atlassian e Internet Systems Consortium (ISC) han revelado varias fallas de seguridad que afectan a sus productos y que podrían explotarse para lograr denegación de servicio (DoS) y ejecución remota de código.

Estado

El proveedor australiano de servicios de software informó que los cuatro fallos de alta gravedad se solucionaron en las nuevas versiones enviadas el mes pasado. Esto incluye:

1. Con una puntuación CVSS de 7,5: una falla de deserialización en el paquete Google Gson que afecta la administración de parches en el servidor y el centro de datos de Jira Service Management
2. Con una puntuación CVSS de 7,5: una falla DoS en el centro de datos y el servidor de Confluence
3. Con una puntuación CVSS de 8,5: una falla de RCE en el servidor y el centro de datos de Bitbucket
4. Con una puntuación CVSS de 7,5: una falla DoS en el servidor Apache Tomcat que afecta al servidor y al centro de datos de Bamboo

Las fallas se han solucionado en las siguientes versiones:

1. Jira Service Management Server y Data Center (versiones 4.20.25, 5.4.9, 5.9.2, 5.10.1, 5.11.0 o posteriores)
2. Confluence Server y Data Center (versiones 7.19.13, 7.19.14, 8.5.1, 8.6.0 o posteriores)
3. Bitbucket Server y Data Center (versiones 8.9.5, 8.10.5, 8.11.4, 8.12.2, 8.13.1, 8.14.0 o posteriores)

4. Bamboo Server y Data Center (versiones 9.2.4, 9.3.1 o posteriores)

Se corrigieron dos fallas de alta gravedad en BIND#

En un desarrollo relacionado, ISC ha publicado correcciones para dos errores de alta gravedad que afectan el paquete de software Berkeley Internet Name Domain (BIND) 9 Domain Name System (DNS) que podrían allanar el camino para una condición DoS:

Con una puntuación CVSS: 7,5: una falla de agotamiento de la pila en el código del canal de control puede provocar que el nombre finalice inesperadamente (corregido en las versiones 9.16.44, 9.18.19, 9.19.17, 9.16.44-S1 y 9.18). .19-S1)

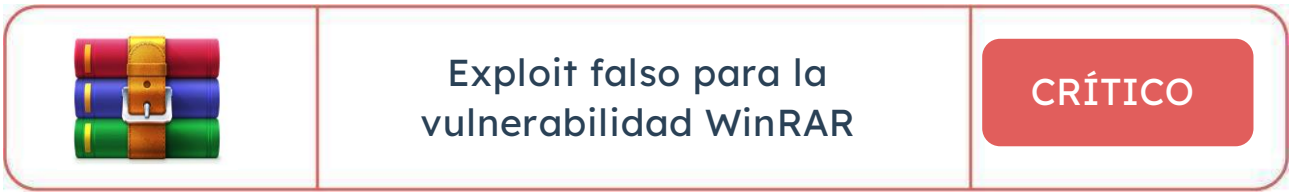
Con una puntuación CVSS: 7,5: el servicio nombrado puede finalizar inesperadamente bajo una carga alta de consultas DNS sobre TLS (corregido en las versiones 9.18.19 y 9.18.19-S1).

Los últimos parches llegan tres meses después de que ISC implementara correcciones para otras tres fallas en el software con puntuaciones CVSS: 7.5 que podrían resultar en una condición DoS.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/09/high-severity-flaws-uncovered-in.html



Descripción

Un actor malicioso lanzó un exploit de prueba de concepto (PoC) falso para una vulnerabilidad WinRAR recientemente revelada en GitHub con el objetivo de infectar a los usuarios que descargaron el código con el malware Venom RAT.

Estado

El PoC falso destinado a explotar esta vulnerabilidad de WinRAR se basó en un script PoC disponible públicamente que explotaba una vulnerabilidad de inyección SQL en una aplicación llamada GeoServer.

Si bien las PoC falsas se han convertido en una táctica bien documentada para atacar a la comunidad de investigación, se sospecha que los actores de amenazas están apuntando

de manera oportunista a otros delincuentes que pueden estar adoptando las últimas vulnerabilidades en su arsenal.

Whalersplonk, la cuenta de GitHub que alojaba el repositorio, ya no es accesible. Se dice que la PoC se cometió el 21 de agosto de 2023, cuatro días después de que se anunciara públicamente la vulnerabilidad. Ésta se relaciona con un problema de validación incorrecta en la utilidad WinRAR que podría explotarse para lograr la ejecución remota de código (RCE) en sistemas Windows. Los mantenedores lo solucionaron el mes pasado en la versión WinRAR 6.23, junto con otra falla explotada activamente.

Un análisis del repositorio revela un script de Python y un vídeo Streamable que demuestra cómo utilizar el exploit. El video atrajo 121 visitas en total.

El script Python, a diferencia de ejecutar PoC, llega a un servidor remoto (checkblacklistwords[.]eu) para recuperar un ejecutable llamado Windows.Gaming.Preview.exe, que es una variante de Venom RAT. Viene con capacidades para enumerar procesos en ejecución y recibir comandos de un servidor controlado por actores (94.156.253[.]109).

Un examen más detenido de la infraestructura del ataque muestra que el actor de la amenaza creó el dominio checkblacklistwords[.]eu al menos 10 días antes de la divulgación pública de la falla, y luego rápidamente aprovechó la importancia del error para atraer víctimas potenciales.

Un actor de amenazas desconocido intentó comprometer a individuos publicando un PoC falso después del anuncio público de la vulnerabilidad, para explotar una vulnerabilidad RCE en una aplicación conocida.

Este PoC es falso y no explota la vulnerabilidad de WinRAR, lo que sugiere que el actor intentó aprovechar un RCE muy buscado en WinRAR para comprometer a otros.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/09/beware-fake-exploit-for-winrar.html

duolingo	Duolingo: 2,6 millones de datos publicados en la dark web	CRÍTICO

Descripción

Los datos fueron extraídos usando una interfaz abierta de planificación de aplicaciones (API).

Estado

Los datos extraídos de más de 2,6 millones de usuarios de la aplicación de aprendizaje de idiomas Duolingo se publicaron en un foro de piratería de la dark web.

La información fue puesta a la venta en un foro de piratería de la dark web el 22 de agosto por un actor malicioso. El actor malicioso ofrecía 1.500 dólares por los 2,6 millones de registros. El pirata informático afirmó haber obtenido acceso a los datos mediante el raspado y la interfaz de aplicación (API) expuesta. También confirmaron la legitimidad de los datos ofreciendo una muestra de los datos de 1.000 cuentas.

Duolingo confirmó al sitio de noticias TheRecord que los datos fueron extraídos de la información del perfil público. Los datos expuestos incluyen nombres de usuarios, nombres de usuario, direcciones de correo electrónico y otra información relevante para los servicios de Duolingo. Es importante señalar, sin embargo, que las direcciones de correo electrónico no son información pública en Duolingo.

Un portavoz de Duolingo dijo sobre el incidente de seguridad cibernética: “No se ha producido ninguna violación o piratería de datos. Nos tomamos en serio la privacidad y la seguridad de los datos y continuamos investigando este asunto para determinar si es necesario tomar medidas adicionales para proteger a nuestros estudiantes”.

La API expuesta es de conocimiento público desde marzo de 2023. Permite a cualquiera recuperar la información pública de cualquier perfil de Duolingo ingresando su nombre de usuario. Se confirmó que la API todavía estaba abierta en agosto de 2023, a pesar de que Duolingo fue alertado de que estaba abierta en enero de 2023. Esto se debió a que un actor malicioso intentó vender en el foro de piratería ahora desaparecido, Breached.

El 1 de septiembre, un portavoz de Duolingo se puso en contacto con la siguiente actualización: "Nuestra investigación confirmó que esto no fue una infracción ni un hackeo; fue una extracción de datos de perfiles públicos de Duolingo. Ningún sistema de Duolingo ni datos privados de usuarios se vieron comprometidos. De todos modos, como medida de precaución hemos tomado algunas medidas para evitar que esto vuelva a suceder.

"Hemos establecido límites de velocidad en el punto final API específico para que sea más difícil para los atacantes abusar de él. Nos tomamos en serio la privacidad y la seguridad de los datos y continuaremos evaluando constantemente nuestras medidas de seguridad para garantizar la seguridad de los estudiantes".

Remediación / Referencias

Por mayor información acceder a:

https://www.cshub.com/data/news/data-of-26-million-duolingo-users-posted-on-the-dark-web

Prevención

Apple parchea 3 nuevos fallos de día cero: iOS, macOS, Safari y más vulnerables

PREVENCIÓN

Descripción

Apple ha lanzado otra ronda de parches de seguridad para abordar tres fallas de día cero explotadas activamente que afectan a iOS, iPadOS, macOS, watchOS y Safari, elevando a 16 el total de errores de día cero descubiertos en su software este año.

Estado

La lista de vulnerabilidades de seguridad es la siguiente:

1. Un problema de validación de certificados en el marco de seguridad que podría permitir que una aplicación maliciosa omita la validación de firmas.
2. Una falla de seguridad en el Kernel que podría permitir a un atacante local elevar sus privilegios.
3. Una falla de WebKit que podría provocar la ejecución de código arbitrario al procesar contenido web especialmente diseñado.

Apple no proporcionó detalles adicionales, salvo un reconocimiento de que "el problema puede haber sido explotado activamente en versiones de iOS anteriores a iOS 16.7".

Las actualizaciones están disponibles para los siguientes dispositivos y sistemas operativos:

- iOS 16.7 y iPadOS 16.7: iPhone 8 y posteriores, iPad Pro (todos los modelos), iPad Air de 3.ª generación y posteriores, iPad de 5.ª generación y posteriores, y iPad mini de 5.ª generación y posteriores
- iOS 17.0.1 y iPadOS 17.0.1: iPhone XS y posteriores, iPad Pro de 12,9 pulgadas de segunda generación y posteriores, iPad Pro de 10,5 pulgadas, iPad Pro de 11 pulgadas de primera generación y posteriores, iPad Air de tercera generación y posteriores, iPad de sexta generación generación y posteriores, iPad mini de 5.ª generación y posteriores
- macOS Monterey 12.7 y macOS Ventura 13.6
- watchOS 9.6.3 y watchOS 10.0.1 - Apple Watch Series 4 y posteriores
- Safari 16.6.1 - macOS Big Sur y macOS Monterey

La divulgación se produce dos semanas después de que Apple resolvió otros dos días cero explotados activamente que se habían encadenado como parte de una cadena de exploits de iMessage de cero clic llamada BLASTPASS para implementar un software espía mercenario conocido como Pegaso.

A esto le siguieron correcciones de envío de Google y Mozilla para contener una falla de seguridad que podría resultar en la ejecución de código arbitrario al procesar una imagen especialmente diseñada.

Hay evidencia que sugiere que tanto la vulnerabilidad de desbordamiento de búfer en el marco de análisis de imágenes Image I/O de Apple, como el desbordamiento de búfer de montón en la biblioteca de imágenes WebP (libwebp), podrían referirse al mismo error, según investigadores de seguridad contratados por le empresa.

En un análisis publicado, revelaron que la biblioteca libwebp se utiliza en varios sistemas operativos, paquetes de software, aplicaciones Linux e imágenes de contenedores, destacando que el alcance de la vulnerabilidad es mucho más amplio de lo que se suponía inicialmente.

"La buena noticia es que el error parece haber sido parcheado correctamente en libwebp, y ese parche está llegando a donde debería ir". "La mala noticia es que libwebp se utiliza en muchos lugares y podría pasar algún tiempo hasta que el parche alcance la saturación", informaron los investigadores.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/09/apple-rushes-to-patch-3-new-zero-day.html

Conclusiones

La evolución digital en el ámbito de la ciberseguridad es un tema de vital importancia en nuestro mundo cada vez más interconectado. Como hemos visto en este boletín de noticias, los ciberdelincuentes están constantemente desarrollando nuevas tácticas y técnicas para comprometer la seguridad de individuos y organizaciones.

Para protegernos en este entorno digital en constante cambio, es esencial estar atentos y tomar medidas proactivas. Esto incluye mantener nuestros sistemas y software actualizados, utilizar contraseñas fuertes y únicas, educarnos sobre las amenazas cibernéticas y practicar la higiene digital en nuestras actividades en línea.

Además, es crucial fomentar la colaboración y la concienciación sobre la ciberseguridad en nuestra sociedad. Las empresas, las instituciones gubernamentales y los ciudadanos deben trabajar juntos para compartir información sobre amenazas y mejores prácticas de seguridad.

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

¡Hasta la próxima!