Boletín de Ciberseguridad

Fecha de Publicación
03/01/2022- N.º 24

Mes de Enero
20/12/2021- 03/01/2022

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 enero se destacan 7 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Errores en Microsoft Teams dejan a la plataforma vulnerable

Atacantes explotan errores en la función de "vista previa del enlace" en Microsoft Teams, pudiendo abusar de los defectos para falsificar enlaces, filtrar direcciones IP y lanzar ataques DoS.

Error en Azure App Service expuso cientos de repositorios de código fuente

Se descubrió una vulnerabilidad en Azure App Service de Microsoft, que ha expuesto el código fuente de las aplicaciones cliente escritas en Java, Node, PHP, Python y Ruby durante al menos cuatro años desde septiembre de 2017.

Actualización de Apache Log4j para parchear nueva vulnerabilidad

La Apache Software Foundation lanzó nuevos parches para contener una falla de ejecución de código arbitrario en Log4j que podría ser abusada por los actores de amenazas para ejecutar código malicioso en los sistemas afectados, lo que la convierte en la quinta deficiencia de seguridad descubierta en la herramienta en el lapso de un mes.

Shutterfly	**Shutterfly reporta un incidente de ransomware**	CRÍTICO

Descripción

La empresa de imágenes digitales *Shutterfly* anunció que ha sido atacada por el grupo de ransomware *Conti*.

Estado

Shutterfly informó en un comunicado que sus divisiones comerciales *Lifetouch* y *BorrowLenses* se vieron afectadas. También han experimentado interrupciones en *Groovebook*, escritorios de producción y algunos sistemas corporativos.

Actualmente se está llevando a cabo una investigación para evaluar el alcance total de los datos afectados, teniendo como prioridad clave su comprensión. Asimismo, la compañía asegura que la información de tarjetas de crédito, cuentas financieras o similares no son almacenados, por lo que esta información no se vió afectada en este incidente.

El grupo *Conti* es el primer grupo sofisticado de ciberdelincuentes descubierto, que ha forjado un nombre al atacar a cientos de instituciones de atención médica, incluyendo ataques ransomware debilitantes contra los Servicios de Salud de Irlanda, Universidad de Utah y otras organizaciones gubernamentales como el gobierno de la ciudad de Tulsa-Oklahoma y la Agencia de Protección Ambiental de Escocia.

Investigadores señalan que analizando la muestra de ransomwares protagonizados por *Conti,* se observa una ganancia de más de $150 millones de dólares en los últimos seis meses.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos y el FBI establecen que se han registrado más de 400 ataques de ransomware relacionados con este grupo de cibercriminales, contra organizaciones estadounidenses y empresas internacionales. El FBI ha implicado previamente a *Conti* en ataques contra al menos 290 organizaciones en Estados Unidos.

Remediación / Referencias

Aún se encuentra en curso la investigación para determinar el número de afectados y evaluar medidas de mitigación.

Por mayor información acceder a:
https://www.zdnet.com/article/shutterfly-reports-ransomware-incident/

	Errores en Microsoft Teams dejan a la plataforma vulnerable	CRÍTICO

Descripción

Atacantes explotan errores en la función de "vista previa del enlace" en Microsoft Teams, pudiendo abusar de los defectos para falsificar enlaces, filtrar direcciones IP y lanzar ataques DoS.

Estado

Microsoft Teams es una herramienta de colaboración que ayuda a las personas que trabajan en diferentes geografías a trabajar juntas en línea. Por esta razón, el uso de la plataforma ha aumentado durante la pandemia, lo que la convierte en un objetivo cada vez más atractivo para los actores de amenazas.

Cuatro vulnerabilidades en Microsoft Teams, sin parches desde marzo, permitieron la suplantación de enlaces de URL y abrieron la puerta a ataques DoS contra usuarios de Android.

Investigadores reportaron estos cuatro errores en la plataforma a principios de este año a Microsoft. Hasta ahora, solo uno de los errores, un error que permite a los atacantes filtrar direcciones IP de Android, fué reparado por la empresa.

Dos de los cuatro errores descubiertos afectaron el uso de Microsoft Teams en cualquier dispositivo y permiten la falsificación de solicitudes del lado del servidor (SSRF) y la suplantación. Los otros dos, denominados "Fuga de direcciones IP" y "Denegación de servicio" afectan solo a los usuarios de Android.

Los atacantes pueden usar el error de suplantación de identidad para reforzar los ataques de phishing u ocultar enlaces maliciosos en el contenido enviado a los usuarios. Esto se puede hacer configurando el destino del enlace de vista previa.

Para abusar del error DoS de Android, un actor de amenazas puede enviar un mensaje a alguien que usa Teams a través de su aplicación de Android que incluye una vista previa del enlace con un objetivo de enlace de vista previa no válido. Esto bloqueará la aplicación continuamente cuando el usuario intente abrir el chat/canal con el mensaje malicioso, básicamente bloqueando a los usuarios fuera del chat o canal.

Por último, los atacantes pueden utilizar el error de fuga de direcciones IP, para interceptar mensajes que incluyen una vista previa del enlace para apuntar la URL en miniatura a un dominio que no es de Microsoft. Esto es posible en las vistas previas de enlaces en las que el backend obtiene la miniatura de la vista previa a la que se hace referencia y la pone a disposición de un dominio de Microsoft.

Remediación / Referencias

Microsoft señaló que se investigaron los cuatro informes y se llegó a la conclusión de que no representan amenazas inmediatas que requieran una corrección de seguridad. Han recibido informes similares en el pasado y se han realizado varias mejoras recientes en el manejo de datos y la seguridad en general. Estos cambios bloquean la reproducción de varios de estos informes, incluida la filtración de direcciones IP informadas sobre el problema de Android.

Para los errores DoS y SSRF, Microsoft determinó que el error DoS no requiere servicio de seguridad inmediato ya que es de baja gravedad para DoS temporal ya que requiere reiniciar la aplicación, pero se considerará solucionar el problema en una versión posterior del producto.

En cuanto al error de SSRF, Microsoft no dio ningún motivo para cerrar el caso sin un parche, y solo informó que la compañía no solucionaría esta vulnerabilidad en la versión actual.

Microsoft también se negó a parchear la fuga de la dirección IP de Android, determinando que el problema no representa una amenaza inmediata que requiera atención urgente, debido a la sensibilidad general de los datos de la dirección IP.

Puedes acceder a toda la información en el siguiente enlace:
https://thecybersecurity.news/vulnerabilities/four-bugs-in-microsoft-teams-left-platform-vulnerable-since-march-15515/

Microsoft Azure	Error en Azure App Service expuso cientos de repositorios de código fuente	CRÍTICO

Descripción

Se descubrió una vulnerabilidad en Azure App Service de Microsoft, que ha expuesto el código fuente de las aplicaciones cliente escritas en Java, Node, PHP, Python y Ruby durante al menos cuatro años desde septiembre de 2017.

Estado

Azure App Service (también conocido como Azure Web Apps) es una plataforma basada en la computación en la nube para crear y alojar aplicaciones web. Permite a los usuarios implementar código fuente y artefactos en el servicio mediante un repositorio de Git local o mediante repositorios alojados en *GitHub* y *Bitbucket*.

El comportamiento inseguro ocurre cuando se usa el método Local Git para implementar en Azure App Service, lo que da como resultado un escenario en el que el repositorio Git se crea dentro de un directorio de acceso público (home / site / wwwroot).

Si bien Microsoft agrega un archivo "web.config" a la carpeta.git, que contiene el estado y el historial del repositorio, para restringir el acceso público, los archivos de configuración solo se usan con aplicaciones C # o ASP.NET que dependen de las propias de Microsoft. Servidores web IIS, dejando fuera las aplicaciones codificadas en otros lenguajes de programación como PHP, Ruby, Python o Node que se implementan con diferentes servidores web como Apache, Nginx y Flask.

Los actores malintencionados escanean continuamente Internet en busca de carpetas Git expuestas de las que puedan recopilar secretos y propiedad intelectual. Además de la posibilidad de que la fuente contenga información sensible como contraseñas y tokens de acceso, el código fuente filtrado a menudo se usa para ataques más sofisticados.

Remediación / Referencias

La compañía informó que un subconjunto limitado de clientes está en riesgo, y agregó que los clientes que implementan código en App Service Linux a través de Local Git después de que los archivos fueran creados en la aplicación fueron los únicos clientes afectados.

Microsoft envió diferentes notificaciones por correo electrónico a todos los usuarios afectados según su configuración en diciembre de 2021.

Cómo comprobar si la aplicación es susceptible a este problema:
Una solicitud HTTP al URL "/.git./HEAD" desde la aplicación devuelve el contenido del archivo "HEAD" en /home/site/wwwroot/.git/HEAD. Si la aplicación no devuelve el contenido del archivo, se confirma que el código fuente no es accesible externamente. Asimismo se recomienda realizar

actualizaciones en la aplicación web, para que la carpeta .git se migre a la carpeta repositorio como defensa.

Para resolverlo:
Asegúrese de realizar copias de seguridad de su aplicación web antes de crear una instancia de cualquier proceso de migración.
Siga las instrucciones en:
https://github.com/projectkudu/kudu/wiki/Deploying-inplace-and-without-repository#how-to-turn-off-in-place-deployment para desactivar las implementaciones in situ.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2021/12/4-year-old-bug-in-azure-app-service.html

Itaú	**Malware de Android dirigido a clientes de Banco Itaú Brasil**	CRÍTICO

Descripción

Investigadores han descubierto un nuevo malware Android dirigido al Banco Itaú Brasil que utiliza páginas similares a Google Play Store para realizar transacciones financieras fraudulentas en los dispositivos de las víctimas.

Estado

Esta aplicación tiene un icono y un nombre similar que podría engañar a los usuarios haciéndoles pensar que es una aplicación legítima relacionada con Itaú Unibanco.
Los cibercriminales han creado una página falsa de Google Play Store y ha alojado el malware que apunta a Itaú Unibanco bajo el nombre 'sincronizador.apk'".

En la última instancia observada, la URL falsa no solo se hace pasar por el mercado oficial de aplicaciones de Android, sino que también aloja la aplicación Itaú Unibanco con malware, además de afirmar que la aplicación ha tenido 1.895.897 descargas.

A los usuarios que instalan e inician la aplicación impostora desde la supuesta página de Google Play Store se les solicita posteriormente que habiliten los servicios de accesibilidad, así como otros

permisos intrusivos que permiten que el malware acceda a las notificaciones, recupere el contenido de la ventana y realice gestos de tocar y deslizar.

El objetivo del troyano, según los investigadores, es realizar transacciones financieras fraudulentas en la aplicación legítima Itaú Unibanco manipulando los campos de entrada del usuario, uniéndose a una larga lista de malware bancario que abusan de la API de accesibilidad. Google, por su parte, ha comenzado a imponer nuevas limitaciones para restringir el uso de dichos permisos que permiten a las aplicaciones capturar información sensible de dispositivos Android.

Remediación / Referencias

Los agentes de amenazas adaptan constantemente sus métodos para evitar la detección y encontrar nuevas formas de dirigirse a los usuarios a través de técnicas cada vez más sofisticadas. Estas aplicaciones maliciosas a menudo se hacen pasar por aplicaciones legítimas para engañar a los usuarios para que las instalen.

Los usuarios deben instalar aplicaciones solo después de verificar su autenticidad e instalarlas exclusivamente desde la tienda oficial de Google Play y otros portales confiables para evitar tales ataques.

Accede a la nota completa aquí:
https://thehackernews.com/2021/12/new-android-malware-targeting-brazils_27.html

	Covid Omicron Phishing	IMPORTANTE

Descripción

Los investigadores de seguridad advierten de un aumento en los ataques de phishing con temas relacionados a COVID, Omicron e información de pruebas.

Estado

Los ciberdelincuentes realizan ataques de phishing dirigidos a universidades buscando robar información valiosa, teniendo el objetivo de engañar a los usuarios para que entreguen sus credenciales de inicio de sesión de la universidad (u otras).

Los correos electrónicos enviados de forma masiva, contienen un dominio de correo electrónico extraño y sospechoso, buscando atraer al lector utilizando a Omicron (variante de Covid 19) como mensaje central, ofreciendo un testeo de prevención, obligando al destinatario a seguir un enlace para poder acceder al beneficio.

Remediación / Referencias

Como regla general, manténgase alerta y evalúe los mensajes recibidos con los siguientes consejos de seguridad:

1. No cliquee enlaces. Al recibir enlaces de un correo electrónico sospechoso, realice una búsqueda del URL. Incluso si un sitio web y/o URL en un correo electrónico parecen reales, los delincuentes pueden enmascarar su verdadero destino.
2. Sea escéptico con las solicitudes urgentes. Los mensajes de phishing suelen presentar solicitudes o demandas urgentes. Cuando detecte un tono de urgencia, verifique la autenticidad del remitente y la solicitud utilizando canales oficiales, en lugar de la información proporcionada por el remitente.
3. Mantenga su información privada. Nunca dé sus contraseñas, información de tarjeta de crédito u otra información privada por correo electrónico.

Por mayor información:
https://www.welivesecurity.com/la-es/2021/12/07/estafadores-aprovechan-preocupacion-omicron-una-nueva-campana-phishing/
https://www.avast.com/es-es/c-phishing#gref

Apache LOG4J	**Actualización de Apache Log4j para parchear nueva vulnerabilidad**	PREVENCIÓN

Descripción

La Apache Software Foundation lanzó nuevos parches para contener una falla de ejecución de código arbitrario en Log4j que podría ser abusada por los actores de amenazas para ejecutar código malicioso en los sistemas afectados, lo que la convierte en la quinta deficiencia de seguridad descubierta en la herramienta en el lapso de un mes.

Estado

La vulnerabilidad tiene una severidad de 6.6 en una escala de 10 e impacta todas las versiones de la librería de registro desde 2.0-alpha 7 a 2.17.0 con la excepción de 2.3.2 y 2.12.4.

Dichas versiones se verán vulnerables a un ataque de ejecución remota de código (RCE) en el que un atacante con permiso para modificar el archivo de configuración de registro puede construir una configuración usando un *Appender JDBC* con una fuente de datos que hace referencia a un *URI JNDI* que puede ejecutar código remoto.
Este problema se soluciona limitando los nombres de las fuentes de datos *JNDI* al protocolo java en las versiones 2.17.1, 2.12.4 y 2.3.2 de Log4j2.

La complejidad de esta vulnerabilidad requiere que el atacante tenga control sobre la configuración. A diferencia de Logback, en Log4j hay una función para cargar un archivo de configuración remota

o para configurar el registrador a través del código, por lo que se podría lograr una ejecución de código arbitrario con un ataque MitM, la entrada del usuario termina en una variable de configuración vulnerable, o modificando el archivo de configuración.

Con la última solución, los encargados del mantenimiento del proyecto han abordado un total de cuatro problemas en Log4j desde que la falla de Log4Shell salió a la luz a principios de este mes, sin mencionar una quinta vulnerabilidad que afecta a las versiones Log4j 1.2 que no se solucionará.

Remediación / Referencias

Se debe actualizar Apache Log4j2 a las versiones 2.17.1, 2.12.4 y 2.3.2 o superiores.

Para saber más invitamos a visitar el siguiente sitio:
https://logging.apache.org/log4j/2.x/security.html
https://checkmarx.com/blog/cve-2021-44832-apache-log4j-2-17-0-arbitrary-code-execution-via-jdbcappender-datasource-element/

APACHE HTTP SERVER PROJECT	**Apache actualiza seguridad para HTTP Server**	PREVENCIÓN

Descripción

Lanzan actualización para una falla crítica en Apache HTTP Server, el segundo servidor web más utilizado del mundo. Apache Software Foundation ha lanzado una actualización para abordar una falla crítica en su servidor web enormemente popular que permite a los atacantes remotos tomar el control de un sistema vulnerable.

Estado

La fundación ha lanzado una nueva versión del servidor HTTP Apache (servidor web) que aborda dos fallas con puntajes de criticidad CVSS respectivos de 9.8 (crítico) y 8.2 (alto) de un posible 10.

Esta versión de Apache HTTP Server es la última versión disponible de forma general de la rama de nueva generación 2.4.x de Apache HTTPD, que mantiene un servidor HTTP importante y moderno de código abierto para plataformas Unix y Windows.

Apache HTTP Server es el segundo servidor web más utilizado en Internet detrás de Nginx, que estima que lo utiliza el 31.4% de los sitios web del mundo.

Aun siendo un error crítico, por el momento no se está al tanto de un exploit para esta vulnerabilidad, pero el equipo de HTTPD cree que tiene el potencial de ser armado, ya que un cuerpo de solicitud cuidadosamente elaborado, puede causar un posible desbordamiento del búfer al analizar contenido de varias partes en mod_lua.

El servidor HTTP Apache no se vio afectado directamente por la biblioteca de mensajes de error Log4j basada en Java, ya que estaba escrita en C. Sin embargo, incluso los servidores web escritos en lenguajes distintos de Java pueden haber integrado la librería Log4j vulnerable en su stack tecnológico.

Remediación / Referencias

Las organizaciones y las personas que ejecutan Apache HTTP Server deben actualizar el software a la última versión lo antes posible para protegerse de cualquier ataque potencial que aproveche esta falla crítica.

Por mayor información al respecto se puede acceder a:
https://httpd.apache.org/security/vulnerabilities_24.html
https://www.siasat.com/apache-releases-new-security-patch-for-http-server-2246686/

Conclusiones

En este boletín de fin de año, los mejores deseos para nuestros lectores y con seguridad de un nuevo comienzo.

Destacamos en esta oportunidad algunas temáticas como el monitoreo de sitios, aplicaciones y demás fraudes y falsas empresas que nos quieren imitar, copiar, y así comprometer la información de nuestros usuarios y la organización por completo; existiendo a nivel mundial un trabajo muy eficiente hoy en día para grandes tecnologías y empresas, en las que el monitoreo, reporte rápido y bloqueo de dominios falsos funciona muy bien.
Lo que cada vez es más frecuente en los repositorios de software como Google Play o Apple Store, entre otras.
Su evolución es lenta y recomendamos contar muchas veces con software antivirus, si es que no se hace una revisión de las aplicaciones que se instalan.

En muchas ocasiones y cada vez más, las empresas delegan algunos controles tecnológicos que puedan implementar para la detección y respuesta eficiente, y por otro lado, hay otras que delegan a los usuarios parte de aceptar riesgos en un período de tiempo, pero que posteriormente y muchas veces lo colocan en la hoja de ruta como una mejora para versiones posteriores.
Lo que sin lugar a dudas es relevante, es la conciencia de ciberseguridad, que cada persona de nuestra organización comprenda sobre los mejores usos y prácticas para manejar información de todo tipo y en cualquier situación.

Nuestro ámbito fomenta los aspectos críticos y de escepticismo en general, así como también la empatía y la confianza, ya que asegurando los canales de comunicación podemos fomentar más conexiones, más comercio y más amigos.

Quienes disfruten de sus vacaciones en estos días, tengan mucho en cuenta y cuidado con sus efectos personales, sobre todo el lugar físico de celulares, tablets, laptops. Recomendamos disfrutar mucho y asegurar antes los mismos tanto con respaldos de información, asegurar el acceso y activar o quizá probar los métodos de búsqueda remota que también todos deberíamos tener activados en nuestros dispositivos portátiles.

Desde el equipo de Datasec los mejores deseos, y disfruten con tranquilidad.