Boletín de Ciberseguridad

Fecha de Publicación
20/12/2021- N.º 23

Mes de Diciembre
06/12/2021 - 20/12/2021

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 segunda quincena del mes de diciembre se destacan siete noticias de relevancia: cuatro sobre vulnerabilidades tecnológicas, dos de fraudes activos y dos de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Zero-Day: Log4Shell

Expertos en ciberseguridad descubren una vulnerabilidad zero-day crítica, denominada Log4Shell, especialmente peligrosa por su facilidad de explotación.

Bots de Twitter utilizados para robo carteras digitales

Compañía líder en detección de amenazas, detecta utilización de bots de Twitter para acceder a las carteras digitales de sus usuarios.

Propagación de malware a través de routers inalámbricos TP - Link

El equipo de FortiGuard Labs, descubre vulnerabilidades graves en el modelo de router TL-WR840 EU V5.

Apache LOG4J	**Zero-Day: Log4Shell**	CRÍTICO

Descripción

Expertos en ciberseguridad descubren vulnerabilidad zero-day crítica, denominada *Log4Shell,* especialmente peligrosa por su facilidad de explotación.

Estado

Log4Shell es una vulnerabilidad de software en *Apache Log4j 2*, una popular biblioteca de Java para registrar mensajes de error en aplicaciones. El fallo permite a un atacante remoto tomar el control de un dispositivo en Internet si el dispositivo está ejecutando ciertas versiones de Log4j 2.

Los atacantes pueden aprovechar la falla mediante mensajes de texto para controlar una computadora de forma remota. La Apache Software Foundation, que publica la biblioteca Log4j 2, otorgó a la vulnerabilidad una puntuación CVSS de 10 sobre 10, la puntuación de gravedad más alta, debido a su potencial de explotación generalizada y la facilidad con la que los atacantes malintencionados pueden explotarla. Mientras la mitigación evoluciona y el daño se despliega, los fundamentos de la vulnerabilidad Log4Shell no cambiarán.

Lo que hace que Log4Shell sea tan peligroso es la ubicuidad de la biblioteca Log4j 2. Está presente en las principales plataformas, desde Amazon Web Services hasta VMware, y en servicios grandes

y pequeños. La red de dependencias entre las plataformas y servicios afectados significa que la aplicación de parches puede ser un proceso complejo y posiblemente largo.
La facilidad para explotar la falla agrava su impacto. La biblioteca Log4j 2 controla el modo en que las aplicaciones registran cadenas de código e información. La vulnerabilidad permite a un atacante obtener el control de una cadena y engañar a la aplicación para que solicite y ejecute código malicioso bajo el control del atacante. Los atacantes pueden tomar el control de forma remota de cualquier servicio conectado a Internet que utilice ciertas versiones de la biblioteca Log4j en cualquier parte de la pila de software.

¿Cómo causa daños la vulnerabilidad Log4Shell?

Dado que la biblioteca Log4j 2 puede comunicarse con otras fuentes y servicios de directorio internos, los atacantes pueden alimentar fácilmente a Log4j 2 con comandos maliciosos desde el exterior y hacer que descargue y ejecute código peligroso de fuentes maliciosas.
La forma en que los atacantes pueden explotar Log4j 2 depende de las características específicas del sistema afectado. Hasta ahora, la mayor parte de la actividad maliciosa ha consistido en el escaneo masivo para detectar sistemas vulnerables.
Los atacantes han estado explotando la vulnerabilidad para comprometer la infraestructura de virtualización, instalar y ejecutar ransomware, robar credenciales del sistema, tomar un amplio control de las redes comprometidas y exfiltrar datos, según un informe de Microsoft.

A medida que aumentan los informes sobre la posibilidad de explotar Log4Shell, las posibilidades de actividad maliciosa parecen exponenciales.
Los actores maliciosos pueden ejecutar cualquier código en el sistema atacado, por ejemplo, para acceder a datos de configuración sensibles. Al capturar estos datos, los atacantes podrían obtener el control total de un sistema, y de todos sus datos y aplicaciones.

Remediación / Referencias

Para corregir la vulnerabilidad DoS identificada, los usuarios de Java 8 (y posteriores) deben actualizar Log4j a la versión 2.17.0.

A su vez, se podrán optar por medidas de mitigación en la configuración de la siguiente manera:

- En PatternLayout en la configuración de registro, reemplace las búsquedas de contexto como $ {ctx: loginId} o $$ {ctx: loginId} con patrones de mapa de contexto de subprocesos (% X,% mdc o% MDC).
- De lo contrario, en la configuración, elimine las referencias a búsquedas de contexto como $ {ctx: loginId} o $$ {ctx: loginId} donde se originan en fuentes externas a la aplicación, como encabezados HTTP o entradas del usuario.

Para identificar si contamos con Log4Shell instalado en diferentes sistemas operativos debemos:

- Windows: Ejecutar el siguiente comando en la raíz de C: para ayudar a revelar todos los archivos Log4j: * dir /S /b *log4j*
- Linux: Ejecutar los siguientes comandos:

  * dpkg -l | grep liblog4j
  * dpkg -l | grep log4
  * find / -name log4j-core-*.jar
  * locate log4j | grep -v log4js

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/12/el-ransomware-aprovecha-la.html

tp-link	**Propagación de malware a través de routers inalámbricos TP - Link**	CRÍTICO

Descripción

El equipo de FortiGuard Labs, descubre vulnerabilidades graves en el modelo de router TL-WR840 EU V5.

Estado

El router TP-Link TL-WR840N EU V5 del fabricante es uno de los más vendidos a nivel mundial, por lo cual el número de afectados asciende a miles.

Este fallo de seguridad garantiza al ciberdelincuente la posibilidad de ejecutar comandos arbitrarios al dispositivo de destino, utilizando la botnet denominada MANGA, obligando así a los dispositivos vulnerables a descargar y ejecutar un scrip malicioso el *tshit.sh* que luego descarga la carga útil binaria.

Los clientes que utilicen Fortinet en los equipos con FortiGuard Antivirus estarán protegidos frente a esta amenaza, debido a que el sistema de prevención de intrusiones ya detecta este tipo de ataque y lo bloquea automáticamente.

Remediación / Referencias

Se ha lanzado un firmware solucionando el problema, pero la actualización debe hacerse de forma manual entrando en el router y posteriormente subiendo el firmware.

Si desea saber más al respecto:
https://blog.segu-info.com.ar/2021/12/vulnerabilidad-critica-en-routers-tp.html

FORTINET	**Ejecución de Código Remoto en FortiOs VPN**	CRÍTICO

Descripción

Se identificaron múltiples vulnerabilidades en Fortinet FortiOS. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para activar la ejecución remota de código y la divulgación de información confidencial.

Estado

Un desbordamiento de enteros en la interfaz VPN de FortiGate FortiOS SSL permitirá que partes malintencionadas no autenticadas envíen solicitudes HTTP diseñadas específicamente para ejecutar código arbitrario en el sistema afectado.

Se trata de una vulnerabilidad grave y se le ha otorgado una puntuación CVSS de 8.5 / 10 porque una explotación exitosa permitiría comprometer completamente los sistemas expuestos. La vulnerabilidad radica en las versiones más recientes de FortiOS 6.0.0 y posteriores.

Remediación / Referencias

Se deberá actualizar a FortiOS 7.0.1+, 6.4.6+, FortiOS 6.2.10+ o FortiOS 6.0.13+, pudiendo descargar la actualización del sitio oficial FortiGuard Labs.

https://www.fortiguard.com/psirt/FG-IR-21-049
https://blog.segu-info.com.ar/2021/12/vulnerabilidad-en-ejecucion-remota-de.html

MikroTik	**MikroTik dispositivos siguen siendo vulnerables a las botnets**	CRÍTICO

Descripción

MikroTik es un fabricante letón de enrutadores inalámbricos e ISP que ha vendido más de 2.000.000 de dispositivos en todo el mundo.
Los investigadores han descubierto que demasiados dispositivos siguen siendo vulnerables a tres problemas críticos de ejecución remota de código que pueden llevar a la apropiación total de dispositivos a pesar de todas estas advertencias y ataques.

Estado

La botnet Mēris aprovechó las vulnerabilidades del enrutador MikroTik para crear un ejército de dispositivos que llevaron a cabo un ataque DDoS sin precedentes en Yandex.
Estos dispositivos tienen un poder considerable, lo que los convierte en objetivos atractivos para la minería de criptomonedas y los ataques distribuidos de denegación de servicio (DDoS), a la fecha aproximadamente 300.000 enrutadores MikroTik han sido expuestos a vulnerabilidades críticas.

Remediación / Referencias

Por su parte, MikroTik ha indicado pautas recomendadas para mitigar esta situación:

- Asegurarse de realizar actualizaciones periódicas en los dispositivos.
- En caso de necesitar acceso remoto, utilizar siempre un servicio de VPN seguro.
- Bloquee dominios y puntos finales de túnel asociados con la botnet Meris.
- Utilice contraseñas seguras y modifiquelas de forma regular.

Si desea saber más al respecto:
https://blog.segu-info.com.ar/2021/12/al-menos-300000-dispositivos-mikrotik.html

	Bots de Twitter utilizados para robo de carteras digitales	CRÍTICO

Descripción

Compañía líder en detección de amenazas, detecta utilización de bots de Twitter para acceder a las carteras digitales de sus usuarios.

Estado

Ciberdelincuentes ejecutan campañas de phishing destinadas a robar direcciones de correo electrónico y frases de recuperación de varios monederos digitales haciéndose pasar por representantes de soporte de Twitter.

Para ello, utilizan la API de Twitter, una herramienta totalmente legítima que proporciona acceso en tiempo real a la actividad de las redes sociales y se utiliza para realizar un seguimiento de las palabras específicas. De esta manera, los estafadores pueden identificar inmediatamente a los usuarios que necesitan ayuda o tienen problemas con alguna billetera digital. Luego usan la API para que los bots de Twitter al control de los ciberdelincuentes interactúen con estos usuarios haciéndose pasar por agentes de soporte para ese servicio.

Los mensajes recibidos por este supuesto soporte, incluyen enlaces a falsos formularios de Google Docs y otras plataformas, donde se solicita a la víctima que detalle su problema, así como su dirección de correo electrónico y frase de recuperación de cuenta.

Al proporcionar esta información, los estafadores podrán acceder a los activos almacenados en la billetera, pudiendo así transferirlos a otra billetera bajo su control.

Remediación / Referencias

Twitter informó que están constantemente trabajando para prevenir este tipo de ataques y han prohibido el uso de la API para el envío de spam, obtención de información personal y adquisición de dinero de forma fraudulenta.

Asimismo, se recomienda a los usuarios que nunca compartan su frase de recuperación con nadie. Y de ser posible, activar la verificación de doble autenticación y así sumar una medida de seguridad extra.

Entérate sobre más detalles:
https://www.welivesecurity.com/la-es/2021/12/08/bots-de-twitter-utilizados-en-estafa-que-busca-robar-billeteras-digitales/

BitMart	**Plataforma de criptomonedas BitMart sufre robo de activos**	IMPORTANTE

Descripción

La plataforma de intercambio de criptomonedas BitMart sufrió una brecha en la que los actores de amenazas robaron más de $100 millones de dólares en activos.

Estado

En declaraciones emitidas a través de Telegram, Twitter y la página de soporte de BitMart, el intercambio describió el incidente como "a gran escala" y determinó que estaba relacionado con una de sus carteras calientes Ethereum y Binance Smart Chain, utilizadas para transacciones de criptomonedas. Todas las demás carteras, según el comunicado, están "seguras e ilesas"; sin embargo, los retiros se suspendieron mientras BitMart investiga la infracción.

La causa del incidente fue el robo de una clave privada que permitió el compromiso de las carteras, las cuales están conectadas a Internet y permiten a sus propietarios enviar y recibir criptoactivos.

Luego de la investigación inicial, la plataforma bloqueó la posibilidad de hacer retiros y depósitos, aunque el martes poco a poco comenzaron a habilitarse estas funciones para Ethereum y otros tokens.

Remediación / Referencias

BitMart sigue trabajando para dar solución a esta brecha en su seguridad.
En un tweet publicado por el fundador y CEO de BitMart, Sheldon Xia, aseguró que la compañía utilizará sus fondos para compensar a los usuarios afectados por el incidente.
Puedes acceder a toda la información en el siguiente link:
https://www.welivesecurity.com/la-es/2021/12/09/exchange-bitmart-sufre-robo-150-millones-en-tokens/

Windows 10	**Parche para Malware Emotet en Windows 10**	PREVENCIÓN

Descripción

Microsoft lanza parche para Malware Emotet encontrado en Windows 10, así como para diversas vulnerabilidades de seguridad encontradas.

Estado

Este es un malware / troyano bancario que se instala en el sistema operativo de la computadora, para robar sus datos bancarios cuando intenta acceder a sus cuentas en línea. Una vez que los ciberdelincuentes obtienen sus datos bancarios a través de Emotet, pueden transferir su dinero a otras cuentas bancarias. Es por eso que se recomienda verificar si su PC con Windows está infectada con Emotet y, de ser así, eliminarlo.

Microsoft ha implementado actualizaciones de Patch Tuesday para abordar múltiples vulnerabilidades de seguridad en Windows, incluida una falla explotada activamente que se está abusando para entregar cargas útiles de malware Emotet.

El último lanzamiento mensual de diciembre corrige un total de 67 fallas, lo que eleva el número total de errores parcheados por la compañía este año a 887, según Zero Day Initiative. Siete de las 67 fallas están calificadas como críticas y 60 como importantes en gravedad, y cinco de los problemas se conocen públicamente en el momento de la publicación. Vale la pena señalar que esto se suma a las 21 fallas resueltas en el navegador Microsoft Edge basado en Chromium.

Remediación / Referencias

Los administradores deben instalar inmediatamente los parches publicados en Patch Tuesday de Diciembre de Microsoft para evitar robo de información, entre otros.

Por mayor información al respecto se puede acceder a:
https://www.genbeta.com/actualidad/ultima-actualizacion-para-windows-10-soluciona-67-vulnerabilidades-incluyendo-zero-day-que-propagaba-malware-emotet
https://www.catalog.update.microsoft.com/Search.aspx?q=KB5008212

iOS	**Parche para Remote Jailbreak Exploit en Apple IOS**	PREVENCIÓN

Descripción

En 15 segundos se logró piratear el último, iPhone 13 Pro en el escenario de la Copa Tianfu en Octubre, usando un error del kernel de iOS para el cual Apple ha lanzado parches dando solución a múltiples vulnerabilidades de seguridad, especialmente el *Jailbreak Exploit*.

Estado

Apple lanzó el lunes actualizaciones para iOS, macOS, tvOS y watchOS con parches de seguridad para múltiples vulnerabilidades, incluida una cadena de exploits de fuga remota, así como una serie de problemas críticos en el navegador web Kernel y Safari.

El problema podría haber permitido que una aplicación maliciosa ejecutara código arbitrario con privilegios del kernel. Apple dijo que abordó el error de condición de carrera con "manejo mejorado del estado". La falla también afecta a los dispositivos macOS.

Además se han corregido un total de cinco fallas de Kernel y cuatro IOMobileFrameBuffer (una extensión de kernel para administrar el framebuffer de pantalla) con las últimas actualizaciones.

Remediación / Referencias

Los usuarios deberán instalar manualmente los parches publicados por Apple, así como mantener actualizado su sistema operativo a la última versión disponible.

Por mayor información ingrese:
https://support.apple.com/en-us/HT201222
https://thehackernews.com/2021/12/latest-apple-ios-update-patches-remote.html

Conclusiones

Este fin de año vino cargado de noticias importantes y con gran movimiento en el mundo de la ciberseguridad. Sin lugar a dudas la vulnerabilidad de Apache Log4J de Java es la que está provocando que muchos administradores, desarrolladores y demás equipos de tecnología estén activamente en búsqueda de los sistemas vulnerables y trabajando en la actualización de la librería para resolver el problema crítico de seguridad, ya que esta librería es ampliamente utilizada en numerosos software base que las organizaciones utilizan, y que la explotación es muy sencilla.

A raíz de esto, algo que cada vez tiene más valor es la cadena de suministros, y también el reconocimiento de los componentes y software que tiene la organización, a fin de detectar rápidamente cuales son los activos informáticos afectados, ya que es una muy buena práctica contar con un mapeo de software y versiones utilizadas en los sistemas productivos.

Para empeorar la situación, los actores maliciosos actuaron rápidamente en desarrollar mecanismos como Ransomware para automatizar y obtener los mayores beneficios posibles a través del compromiso masivo de servidores vulnerables.

Muchos clientes comenzaron a solicitarnos servicios y realizar análisis de vulnerabilidades sobre redes internas y externas, de tal forma de detectar y corregir rápidamente para evitar así una ventana de exposición mayor.

Recomendamos a todos nuestros clientes seguir estos lineamientos y trabajar en la actualización de la librería, ya que el impacto podría ser crítico.

Una vez más la correcta gestión y seguimiento de vulnerabilidades, es la que puede marcar en gran medida nuestros éxitos o fracasos en la organización de las tecnologías de la información.

Desde los equipos de Datasec, transmitimos los mejores deseos de prosperidad y éxito para nuestros clientes en este fin de año, dónde comienza un nuevo ciclo lleno de nuevos desafíos en los que estaremos apoyándolos para afrontarlos.

¡Feliz nuevo año!