# Boletín de Ciberseguridad

Fecha de Publicación
24/10/2022 - N.º 45

Mes de Octubre
11/10/2022 -24/10/2022

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 segunda quincena del mes de octubre se destacan 6 noticias de relevancia: cuatro de vulnerabilidades y dos de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

### CISA advierte sobre fallas críticas que afectan Advantech e Hitachi

CISA publicó el martes dos avisos de Sistemas de control industrial (ICS) relacionados con fallas graves en los dispositivos Advantech R-SeeNet y Hitachi Energy APM Edge.

### Zimbra lanza parche para vulnerabilidad de explotación activa

Zimbra ha lanzado parches para contener una falla de seguridad explotada activamente en su suite de colaboración empresarial que podría aprovecharse para cargar archivos arbitrarios en instancias vulnerables.

### Microsoft confirma que hubo una fuga de datos de más de 65 000 empresas

Microsoft confirmó esta semana que sin darse cuenta expuso información relacionada con miles de clientes luego de un lapso de seguridad que dejó un punto final accesible públicamente a través de Internet sin autenticación.


| | | |
|---|---|---|
| APACHE | **Se comenzó a explotar la vulnerabilidad crítica de Apache Commons "Text4Shell"** | CRÍTICO |

## Descripción

La empresa de seguridad de WordPress, Wordfence, dijo el jueves que comenzó a detectar intentos de explotación dirigidos a la falla recientemente revelada en Apache Commons Text el 18 de octubre de 2022.

## Estado

A la vulnerabilidad, rastreada como CVE-2022-42889, también conocida como Text4Shell , se le ha asignado una clasificación de gravedad de 9,8 de un posible 10,0 en la escala CVSS y afecta a las versiones 1.5 a 1.9 de la biblioteca.

Es similar a la ahora infame vulnerabilidad Log4Shell en el sentido de que el problema radica en la forma en que las sustituciones de cadenas realizadas durante las búsquedas de DNS, secuencias de comandos y URL podrían conducir a la ejecución de código arbitrario en sistemas susceptibles al pasar una entrada que no es de confianza.

Una explotación exitosa de la falla puede permitir que un actor de amenazas abra una conexión de shell inversa con la aplicación vulnerable simplemente a través de una carga útil especialmente diseñada, abriendo efectivamente la puerta para ataques de seguimiento.

Si bien el problema se informó originalmente a principios de marzo de 2022, Apache Software Foundation (ASF) lanzó una versión actualizada del software (1.10.0) el 24 de septiembre, y luego emitió un aviso la semana pasada, el 13 de octubre.

**Remediación / Referencias**

Se recomienda a los usuarios que tienen dependencias directas en Apache Commons Text que actualicen a la versión fija para mitigar posibles amenazas. Según Maven Repository , hasta 2593 proyectos usan la biblioteca, aunque Flashpoint señaló que muy pocos de los enumerados usan el método vulnerable.

Puedes acceder a toda la información en el siguiente enlace:
https://www.tarlogic.com/blog/cve-2022-42889-critical-vulnerability-affects-apache-commons-text/

| | | |
|---|---|---|
| cobaltstrike by HelpSystems | **Vulnerabilidad crítica de RCE descubierta en Cobalt Strike** | CRÍTICO |

**Descripción**

Se lanzó una actualización de seguridad fuera de banda para abordar una vulnerabilidad de ejecución remota de código que podría permitir que un atacante tome el control de los sistemas objetivo.

**Estado**

Cobalt Strike es un marco comercial de equipo rojo que se utiliza principalmente para la simulación de adversarios, pero los operadores de ransomware y los grupos de amenazas persistentes avanzadas (APT) centrados en el espionaje han abusado activamente de las versiones descifradas del software.

La herramienta posterior a la explotación consiste en un servidor de equipo, que funciona como un componente de comando y control (C2), y una baliza, el malware predeterminado que se usa para crear una conexión con el servidor de equipo y soltar las cargas útiles de la siguiente etapa.

El problema, rastreado como CVE-2022-42948, afecta a Cobalt Strike versión 4.7.1 y se deriva de un parche incompleto lanzado el 20 de septiembre de 2022 para rectificar una vulnerabilidad de secuencias de comandos entre sitios (XSS) (CVE-2022-39197) que podría conducir a la ejecución remota de código.

Sin embargo, se descubrió que la ejecución remota de código podría activarse en casos específicos utilizando el marco Java Swing, el conjunto de herramientas de interfaz gráfica de usuario que se utiliza para diseñar Cobalt Strike.

Esto significa que un actor malicioso podría explotar este comportamiento por medio de una etiqueta HTML <object>, utilizándose para cargar una carga útil personalizada alojada en un servidor remoto e inyectarla dentro del campo de notas, así como en el menú del explorador de archivos gráficos en Cobalt. interfaz de usuario de huelga.

## Remediación / Referencias

Se descubrió que la ejecución remota de código podría activarse en casos específicos utilizando el marco Java Swing, el conjunto de herramientas de interfaz gráfica de usuario que se utiliza para diseñar Cobalt Strike.

Por mayor información al respecto se puede acceder a:
https://securityintelligence.com/posts/analysis-rce-vulnerability-cobalt-strike/

| | | |
|---|---|---|
| | **CISA advierte sobre fallas críticas que afectan Advantech e Hitachi** | CRÍTICO |

## Descripción

CISA publicó el martes dos avisos de Sistemas de control industrial (ICS) relacionados con fallas graves en los dispositivos Advantech R-SeeNet y Hitachi Energy APM Edge.

## Estado

Esto consiste en tres debilidades en la solución de monitoreo R-SeeNet, cuya explotación exitosa "podría resultar en que un atacante no autorizado elimine archivos en el sistema de forma remota o permita la ejecución remota de código".

La lista de problemas que afectan a las versiones 2.4.17 y anteriores de R-SeeNet es la siguiente:

CVE-2022-3385 y CVE-2022-3386 (puntajes CVSS: 9.8): dos fallas de desbordamiento de búfer basadas en pila que podrían conducir a la ejecución remota de código
CVE-2022-3387 (puntuación CVSS: 6,5): una falla en el recorrido de la ruta que podría permitir que un atacante remoto elimine archivos PDF arbitrarios

Los parches están disponibles en la versión R-SeeNet versión 2.4.21 lanzada el 30 de septiembre de 2022.

CISA también publicó una actualización de un aviso de diciembre de 2021 sobre múltiples fallas en los productos Edge de Hitachi Energy Transformer Asset Performance Management (APM) que podrían volverlos inaccesibles.

**Remediación / Referencias**

Es importante que los propietarios de activos y quienes defienden la infraestructura crítica entiendan cuándo hay soluciones disponibles y cómo se deben implementar y priorizar las mismas.

Por mayor información al respecto se puede acceder a:
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

| | | |
|---|---|---|
| zimbra | **Zimbra lanza parche para vulnerabilidad de explotación activa** | CRÍTICO |

**Descripción**

Zimbra ha lanzado parches para contener una falla de seguridad explotada activamente en su suite de colaboración empresarial que podría aprovecharse para cargar archivos arbitrarios en instancias vulnerables.

**Estado**

Registrado como CVE-2022-41352 (puntuación CVSS: 9,8), el problema afecta a un componente de la suite Zimbra llamado Amavis , un filtro de contenido de código abierto y, más específicamente, a la utilidad cpio que utiliza para escanear y extraer archivos.

A su vez, se dice que la falla tiene sus raíces en otra vulnerabilidad subyacente (CVE-2015-1197 ) que se reveló por primera vez a principios de 2015, que según Flashpoint se rectificó, solo para revertirse posteriormente en distribuciones de Linux posteriores.
Todo lo que un adversario debe hacer para convertir la deficiencia en un arma es enviar un correo electrónico con un archivo adjunto TAR especialmente diseñado que, una vez recibido, se envía a Amavis, que utiliza el módulo cpio para desencadenar el exploit.

**Remediación / Referencias**

Las correcciones están disponibles en las siguientes versiones:

- Zimbra 9.0.0 Parche 27
- Zimbra 8.8.15 Parche 34

Por mayor información al respecto se puede acceder a:
https://blog.zimbra.com/2022/10/new-zimbra-patches-9-0-0-patch-27-8-8-15-patch-34/


| | | |
|---|---|---|
| Microsoft | **Microsoft confirma que hubo una fuga de datos de más de 65 000 empresas** | PREVENCIÓN |

**Descripción**

Microsoft confirmó esta semana que sin darse cuenta expuso información relacionada con miles de clientes luego de un lapso de seguridad que dejó un punto final accesible públicamente a través de Internet sin autenticación.

**Estado**

"Esta mala configuración resultó en el potencial de acceso no autenticado a algunos datos de transacciones comerciales correspondientes a las interacciones entre Microsoft y posibles clientes, como la planificación o la posible implementación y provisión de servicios de Microsoft", dijo Microsoft en una alerta.

Microsoft también enfatizó que la fuga B2B fue "causada por una configuración incorrecta no intencional en un punto final que no está en uso en todo el ecosistema de Microsoft y no fue el resultado de una vulnerabilidad de seguridad".

La configuración incorrecta de Azure Blob Storage fue detectada el 24 de septiembre de 2022 por la empresa de ciberseguridad SOCRadar, que denominó la fuga BlueBleed . Microsoft dijo que está en proceso de notificar directamente a los clientes afectados.

No se reveló la magnitud de la fuga de datos, pero según SOCRadar, afecta a más de 65.000 entidades en 111 países. La exposición asciende a 2,4 terabytes de datos que consisten en facturas, pedidos de productos, documentos de clientes firmados, detalles del ecosistema de socios, entre otros.

Sin embargo, Microsoft ha cuestionado el alcance del problema, afirmando que los datos incluían nombres, direcciones de correo electrónico, contenido de correo electrónico, nombre de la empresa y números de teléfono, y archivos adjuntos relacionados con negocios "entre un cliente y Microsoft o un socio autorizado de Microsoft".

**Remediación / Referencias**

No hay evidencia de que los actores de amenazas accedieron indebidamente a la información antes de la divulgación, pero dichas filtraciones podrían explotarse con fines maliciosos, como extorsión, ataques de ingeniería social o una ganancia rápida.

Puedes acceder a toda la información en el siguiente enlace:
https://learn.microsoft.com/es-es/mem/intune/protect/data-leak-prevention

| | | |
|---|---|---|
| Google | **Google lanza el proyecto de código abierto GUAC** | PREVENCIÓN |

**Descripción**

Google anunció el jueves que está buscando colaboradores para una nueva iniciativa de código abierto llamada Graph for Understanding Artifact Composition , también conocida como GUAC, como parte de sus esfuerzos continuos para reforzar la cadena de suministro de software.

**Estado**

La cadena de suministro de software se ha convertido en un vector de ataque lucrativo para los actores de amenazas, en el que explotar solo una debilidad, como se vio en el caso de SolarWinds y Log4Shell, abre un camino lo suficientemente largo como para atravesar la cadena de suministro y robar datos confidenciales, plantar malware, y tomar el control de los sistemas pertenecientes a clientes intermedios.

Google, el año pasado, lanzó un marco llamado SLSA (abreviatura de Niveles de cadena de suministro para artefactos de software) que tiene como objetivo garantizar la integridad de los paquetes de software y evitar modificaciones no autorizadas.

También lanzó una versión actualizada de Security Scorecards, que identifica el riesgo que las dependencias de terceros pueden introducir en un proyecto, lo que permite a los desarrolladores tomar decisiones informadas sobre la aceptación de código vulnerable o la consideración de otras alternativas.

**Remediación / Referencias**

El objetivo no es solo permitir que las organizaciones determinen si están afectadas por una vulnerabilidad específica, sino también estimar el radio de explosión en caso de que la cadena de suministro se vea comprometida.

Por mayor información:
https://security.googleblog.com/2022/10/announcing-guac-great-pairing-with-slsa.html

## Conclusiones

Las nuevas noticias nos sitúan en un panorama de tendencias, en dónde acudimos a la redefinición del alcance que tiene la ciber resiliencia para todas las tecnologías utilizadas por la humanidad.
Así como evolucionan los ataques, lo hacemos también en la evolución de la respuesta a incidentes y las conversaciones sobre las estrategias.

Nos aprovechamos cada día más de la automatización, y la seguridad también está yendo a una consolidación de proveedores, dónde claramente los productos y servicios de seguridad están convergiendo;
Los proveedores están consolidando las funciones de seguridad en plataformas únicas e introduciendo opciones de precios y licencias para hacer más atractivas las soluciones empaquetadas.

Aunque esto puede introducir nuevos desafíos, como la reducción de la capacidad de negociación y el potencial de puntos únicos de fallo, la consolidación es una tendencia positiva que debería reducir la complejidad, recortar los costes y mejorar la eficiencia, lo que resultaría en una mayor seguridad general.

Los directores de seguridad y gestión del riesgo deben asociarse con otros departamentos para dar prioridad al riesgo de la cadena de suministro digital y presionar a los proveedores para que demuestren las buenas prácticas de seguridad.
Vemos como las grandes organizaciones están trabajando activamente en este ecosistema, en el que necesitamos de más seguridad para evolucionar apropiadamente.
La retroalimentación aporta valor a través de estas consolidaciones de confianza.

Hasta la próxima quincena de noticias.
¡Naveguen seguros!