Boletín de Ciberseguridad

Fecha de Publicación
21/11/2022 - N.º 46

Mes de Noviembre
24/10/2022 - 21/11/2022

Datasec

Índice

Vulnerabilidad crítica

Introducción 2

URLScan filtra inadvertidamente URL y datos confidenciales 3

Medibank se niega a pagar rescate de ransomware: 9.7 millones de clientes expuestos. 5

Múltiples vulnerabilidades reportadas en el software de monitoreo de infraestructura de TI Checkmk. 6

Dropbox: Ciberdelincuentes acceden a 130 repositorios de código fuente de GitHub. 7

Prevención

Azov Ransomware: limpiador que destruye datos de 666 bytes a la vez 8

OpenSSL parchea 2 nuevas vulnerabilidades de alta gravedad 11

Vulnerabilidad crítica en ConnectWise Server Backup Solution 13

Conclusiones 14

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 7 noticias de relevancia: cinco de vulnerabilidades y dos de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Dropbox: Ciberdelincuentes acceden a 130 repositorios de código fuente de GitHub.

El servicio de alojamiento de archivos Dropbox reveló que fué víctima de una campaña de phishing que permitió a actores de amenazas no identificados, obtener acceso no autorizado a de sus repositorios de código fuente en GitHub.

URLScan filtra inadvertidamente URL y datos confidenciales

Investigadores de Seguridad advierten sobre la filtración de información confidencial a través de urlscan.io, un escáner de sitios web utilizado para comprobar URL sospechosas y maliciosas.

Vulnerabilidad crítica en ConnectWise Server Backup Solution

La plataforma de software de gestión de servicios de TI ConnectWise ha lanzado parches de software para una vulnerabilidad de seguridad crítica en Recovery R1Soft Server Backup Manager (SBM).

urlscan.io A sandbox for the web	**URLScan filtra inadvertidamente URL y datos confidenciales**	CRÍTICO

Descripción

Investigadores de Seguridad advierten sobre la filtración de información confidencial a través de urlscan.io, un escáner de sitios web utilizado para comprobar URL sospechosas y maliciosas.

Estado

Las URL sensibles a documentos compartidos, páginas de restablecimiento de contraseña, invitaciones de equipo, facturas de pago y más se enumeran públicamente y se pueden buscar.

Se inició una investigación a raíz de una notificación enviada por GitHub en febrero de 2022 a un número desconocido de usuarios sobre compartir sus nombres de usuario y nombres de repositorios privados (es decir, URL de páginas de GitHub) a urlscan.io para metadatos análisis como parte de un proceso automatizado.
Urlscan.io, que se ha descrito como una caja de arena para la web, está integrado en varias soluciones de seguridad a través de su API.

Con el tipo de integración de esta API (por ejemplo, a través de una herramienta de seguridad que escanea todos los correos electrónicos entrantes y realiza un escaneo de URL en todos los enlaces)

y la cantidad de datos en la base de datos, hay una gran variedad de datos confidenciales que pueden ser buscados y recuperados por un usuario anónimo.

Esto incluye enlaces de restablecimiento de contraseña, enlaces de cancelación de suscripción de correo electrónico, URL de creación de cuentas, claves API, información sobre bots de Telegram, solicitudes de firma de DocuSign, enlaces compartidos de Google Drive, transferencias de archivos de Dropbox, enlaces de invitación a servicios como SharePoint, Discord y Zoom, facturas de PayPal, Grabaciones de reuniones de Cisco Webex e incluso direcciones URL para el seguimiento de paquetes.

Además de eso, el análisis también encontró que las herramientas de seguridad mal configuradas envían cualquier enlace recibido por correo como un escaneo público a urlscan.io.

Esto podría tener graves consecuencias en las que un actor malintencionado puede activar enlaces de restablecimiento de contraseña para las direcciones de correo electrónico afectadas y explotar los resultados del análisis para capturar las URL y hacerse cargo de las cuentas restableciendo la contraseña que elija el atacante.

Para maximizar la efectividad de tal ataque, el adversario puede buscar sitios de notificación de violación de datos como *Have I Been Pwned* para determinar los servicios exactos que se registraron utilizando las direcciones de correo electrónico en cuestión.

Remediación / Referencias

Urlscan.io, luego de la divulgación instó a los usuarios a comprender las diferentes visibilidades de escaneo, revisar sus propios escaneos en busca de información no pública, revisar sus flujos de trabajo de envío automatizado, y hacer cumplir una visibilidad de escaneo máxima para su cuenta.

También ha agregado reglas de eliminación para eliminar regularmente escaneos pasados y futuros que coincidan con los patrones de búsqueda, indicando que tiene listas de bloqueo de patrones de dominio y URL para evitar el escaneo de sitios web particulares.

Esta información podría ser utilizada por los spammers para recopilar direcciones de correo electrónico y otra información personal, los ciberdelincuentes podrían usarlo para apoderarse de cuentas y ejecutar campañas de phishing creíbles.

Puedes acceder a toda la información en el siguiente enlace:
https://thehackernews.com/2022/11/experts-find-urlscan-security-scanner.html

medibank	Medibank se niega a pagar rescate de ransomware	CRÍTICO

Descripción

La aseguradora de salud australiana Medibank confirmó que se accedió a los datos personales pertenecientes a alrededor de 9,7 millones de sus clientes luego de un incidente de ransomware.

Estado

Según la empresa, el ataque se detectó en su red el 12 de octubre de una manera que era coherente con los precursores de un evento de ransomware, lo que la llevó a aislar sus sistemas, pero no antes de que los atacantes extrajeran los datos.

La cifra de clientes afectados representa alrededor de 5,1 millones de clientes de Medibank, alrededor de 2,8 millones de clientes de Ahm y alrededor de 1,8 millones de clientes internacionales.

Medibank declaró que no pagaría ningún rescate al actor de amenazas, afirmando que hacerlo sólo alentaría al atacante a extorsionar a sus clientes y haría de Australia un objetivo más grande. Tras esta declaración el actor de amenazas detrás del incidente de seguridad ha publicado archivos en la web oscura que contienen datos de clientes robados de sus sistemas.

Los detalles comprometidos incluyen nombres, fechas de nacimiento, direcciones, números de teléfono y direcciones de correo electrónico, así como números de Medicare para clientes de ahm y números de pasaporte y detalles de visa para clientes estudiantes internacionales.

La empresa informó que la información financiera y los documentos de identidad, como las licencias de conducir, no se han desviado como parte de la brecha de seguridad y que no se observó actividad inusual.

Si bien la compañía australiana aún no ha atribuido el ataque a un grupo de ransomware específico, los datos se publicaron en un portal web oscuro vinculado a REvil, que relanzó sus operaciones a principios de mayo.

Remediación / Referencias

La empresa indica que, dada la naturaleza del delito, se cree que todos los datos de los clientes a los que se accedió podrían haber sido tomados por los ciberdelincuentes, instando a éstos a estar alerta ante posibles filtraciones.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/11/medibank-refuses-to-pay-ransom-after-97.html

checkmk	**Múltiples vulnerabilidades reportadas en el software de monitoreo de infraestructura de TI Checkmk.**	CRÍTICO

Descripción

CISA advierte fallas graves relacionadas a los dispositivos Advantech R-SeeNet y Hitachi Energy APM Edge de Checkmk.

Estado

Se han revelado múltiples vulnerabilidades en el software de monitoreo de infraestructura de TI que podrían ser encadenadas por un atacante remoto no autenticado para apoderarse por completo de los servidores afectados.

La edición de código abierto de Checkmk de la herramienta de monitoreo se basa en Nagios Core y ofrece integraciones con NagVis para la visualización y generación de mapas topológicos de infraestructuras, servidores, puertos y procesos.

Según sus desarrolladores, sus ediciones Enterprise y Raw son utilizadas por más de 2000 clientes, incluidos Airbus, Adobe, NASA, Siemens, Vodafone y otros.

Las cuatro vulnerabilidades, que consisten en dos errores críticos y dos de gravedad media, son las siguientes:

- Una falla de inyección de código en auth.php de watolib (CVSS: 9.1).
- Una falla de lectura de archivo arbitraria en NagVis (CVSS: 9.1).
- Una falla de inyección de comandos en el envoltorio Livestatus de Checkmk y la API de Python (CVSS: 6.8).
- Una falla de falsificación de solicitud del lado del servidor (SSRF) en la API de registro del host (CVSS: 5.0).

Si bien estas deficiencias por sí solas tienen un impacto limitado, un adversario puede encadenar los problemas, comenzando con la falla SSRF para acceder a un punto final solo accesible desde localhost, usándolo para eludir la autenticación y leer un archivo de configuración, y finalmente obtener acceso a la GUI de Checkmk.

Este acceso se puede convertir aún más en la ejecución remota de código al explotar una vulnerabilidad de inyección de código en un subcomponente de la GUI de Checkmk llamado watolib, que genera un archivo llamado auth.php requerido para la integración de NagVis.

Remediación / Referencias

Tras la divulgación responsable, las cuatro vulnerabilidades se han parcheado en la versión 2.1.0p12 de Checkmk.

Los hallazgos siguen al descubrimiento de múltiples fallas en otras soluciones de monitoreo como Zabbix e Icinga, que podrían haberse aprovechado para comprometer los servidores mediante la ejecución de código arbitrario.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/11/multiple-vulnerabilities-reported-in.html

Dropbox	**Dropbox: Ciberdelincuentes acceden a 130 repositorios de código fuente de GitHub**	CRÍTICO

Descripción

El servicio de alojamiento de archivos Dropbox reveló que fué víctima de una campaña de phishing que permitió a actores de amenazas no identificados, obtener acceso no autorizado a de sus repositorios de código fuente en GitHub.

Estado

Estos repositorios incluían copias de bibliotecas de terceros ligeramente modificadas para su uso por Dropbox, prototipos internos y algunas herramientas y archivos de configuración utilizados por el equipo de seguridad.

La violación resultó en el acceso a algunas claves de API utilizadas por los desarrolladores de Dropbox, así como a miles de nombres y direcciones de correo electrónico pertenecientes a empleados de Dropbox, clientes actuales y anteriores, clientes potenciales de ventas y proveedores.

Sin embargo, enfatizó que los repositorios no contenían código fuente relacionado con sus aplicaciones o infraestructura principales.

Dropbox, que ofrece servicios de almacenamiento en la nube, copia de seguridad de datos y firma de documentos, entre otros, tiene más de 17,37 millones de usuarios de pago y 700 millones de usuarios registrados en agosto de 2022.

La divulgación se produce más de un mes después de que tanto GitHub como CircleCI advirtieran sobre ataques de phishing diseñados para robar credenciales de GitHub a través de notificaciones falsas que pretendían ser de la plataforma CI/CD.

La firma señaló que múltiples usuarios de Dropbox recibieron correos electrónicos de phishing que se hacían pasar por CircleCI a principios de octubre, algunos de los cuales se deslizaron a través de sus filtros automatizados de correo no deseado para llegar a las bandejas de entrada de correo electrónico de los empleados.

Estos correos electrónicos de aspecto legítimo dirigían a los empleados a visitar una página de inicio de sesión falsa de CircleCI, ingresar su nombre de usuario y contraseña de GitHub y luego usar su clave de autenticación de hardware para pasar una contraseña de un solo uso (OTP) al sitio malicioso.

La compañía no reveló cuántos de sus empleados cayeron en el ataque de phishing, pero sí confirmó que tomó medidas inmediatas para rotar todas las credenciales de desarrollador expuestas y que alertó a las autoridades policiales.

También informó que no encontró evidencia de robo de datos de clientes como resultado del incidente, y agregó que está actualizando sus sistemas de autenticación de dos factores para admitir claves de seguridad de hardware para la resistencia al phishing.

Remediación / Referencias

Incluso el profesional más escéptico y vigilante puede ser víctima de un mensaje cuidadosamente elaborado y entregado de la manera correcta en el momento adecuado, esta es precisamente la razón por la que el phishing sigue siendo tan efectivo.

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/11/dropbox-breach-hackers-unauthorizedly.html

Azov Ransomware	**Azov Ransomware: limpiador que destruye datos de 666 bytes a la vez**	CRÍTICO

Descripción

Un nuevo y destructivo limpiador de datos 'Azov Ransomware' se está distribuyendo en gran medida a través de software pirateado, generadores de claves y paquetes de adware, tratando de enmarcar a reconocidos investigadores de seguridad al afirmar que están detrás del ataque.

Estado

El ransomware Azov afirma falsamente haber sido creado por un grupo de reconocidos investigadores de seguridad.

La nota de rescate, llamada RESTORE_FILES.txt, dice que los dispositivos están encriptados en protesta por la toma de Crimea y porque los países occidentales no están haciendo lo suficiente para ayudar a Ucrania en su guerra contra Rusia.

La nota de rescate les dice a las víctimas que se comuniquen con los investigadores detallados en la nota de rescate, a través de Twitter para recuperar archivos, lo que implica falsamente que somos parte de la operación de ransomware.

Este limpiador toma su nombre del Regimiento Azov de Ucrania, una controvertida fuerza militar que supuestamente se asoció con la ideología neonazi en el pasado.

En una campaña iniciada en los últimos días, un actor de amenazas parece haber comprado "instalaciones" a través de la botnet de malware SmokeLoader para entregar el nuevo limpiador destructivo Azov.

SmokeLoader es una botnet de malware que otros actores de amenazas pueden alquilar o comprar 'instalaciones' para distribuir su propio malware en dispositivos infectados. SmokeLoader se distribuye comúnmente a través de sitios web que promueven cracks de software falsos, modificaciones de juegos, trucos y generadores de claves.

En los últimos días, SmokeLoader ha comenzado a entregar el nuevo 'Azov Ransomware', junto con otro malware [VirusTotal], como el malware de robo de información RedLine Stealer y el ransomware STOP.

El ejecutable inicial del ransomware [VirusTotal] se colocará en un archivo aleatorio en la carpeta temporal de Windows (%Temp%) y se ejecutará.

Una vez iniciado, el limpiador copiará C:\Windows\System32\msiexec.exe en C:\ProgramData\rdpclient.exe [VirusTotal] y lo parcheará para que también contenga el limpiador Azov. Además, el limpiador se puede configurar para que se inicie cuando Windows comience a usar la siguiente clave de registro.

El limpiador ahora escaneará todas las unidades de la computadora y encriptará cualquier archivo que no tenga las extensiones .ini, .dll y .exe.

Al cifrar archivos, agregará la extensión de archivo. azov a los nombres de los archivos cifrados. Por ejemplo, 1.doc se cifra y se renombra a 1.doc.azov, como se muestra a continuación.

En cada carpeta que se escanea en busca de archivos, el limpiador creará archivos de texto llamados RESTORE_FILES.txt que contienen un mensaje del actor de amenazas mencionado anteriormente.

Remediación / Referencias

Si bien los investigadores analizarán el ransomware en busca de debilidades en el cifrado, en este momento, el ransomware debe considerarse destructivo, ya que no hay forma de contactar a los actores de la amenaza y recuperar las claves de descifrado.

Sin embargo, si este limpiador de datos cifró sus datos, es probable que también estuviera infectado con otro malware, como troyanos que roban información.

Por lo tanto, debe cambiar de inmediato las contraseñas de sus cuentas en línea, especialmente las de carácter confidencial, como la banca en línea, los administradores de contraseñas y las cuentas de correo electrónico.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2022/11/azov-ransomware-wiper-sin-recuperacion.html

OpenSSL Cryptography and SSL/TLS Toolkit	**OpenSSL parchea 2 nuevas vulnerabilidades de alta gravedad**	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

El proyecto OpenSSL ha implementado correcciones para contener dos fallas de alta gravedad en su biblioteca de criptografía ampliamente utilizada que podría resultar en una denegación de servicio (DoS) y ejecución remota de código.

Se han descrito como vulnerabilidades de saturación de búfer que pueden activarse durante la verificación del certificado X.509 al proporcionar una dirección de correo electrónico especialmente diseñada.

En un cliente TLS, esto puede activarse al conectarse a un servidor malicioso. En un servidor TLS, esto puede activarse si el servidor solicita la autenticación del cliente y se conecta un cliente malintencionado.

OpenSSL es una implementación de código abierto de los protocolos SSL y TLS que se utilizan para la comunicación segura y está integrado en varios sistemas operativos y una amplia gama de software.

Las versiones 3.0.0 a 3.0.6 de la biblioteca se ven afectadas por las nuevas fallas, que se remediaron en la versión 3.0.7. Vale la pena señalar que las versiones de OpenSSL 1.x comúnmente implementadas no son vulnerables.

Según los datos compartidos, se estima que alrededor de 7062 hosts ejecutan una versión susceptible de OpenSSL, con la mayoría de ellos ubicados en los EE. UU., Alemania, Japón, China, Chequia, el Reino Unido, Francia, Rusia, Canadá y los Países Bajos.

Investigadores de seguridad informan que la capacidad de explotación es significativamente limitada, ya que las fallas ocurren después de la verificación del certificado y requiere que una CA haya firmado el certificado malicioso o que la aplicación continúe con la verificación del certificado a pesar de no poder construir una ruta hacia un emisor confiable.

La segunda vulnerabilidad parcheada, se trata de un problema grave de manejo de memoria en la implementación de la extensión de latido TLS/DTLS, permitió a los atacantes leer partes de la memoria de un servidor de destino.

Una vulnerabilidad crítica en una biblioteca de software como OpenSSL, que se usa tanto y es tan fundamental para la seguridad de los datos en Internet, es algo que ninguna organización puede permitirse pasar por alto.

Dicho esto, OpenSSL advirtió que la vulnerabilidad puede ser crítica para los sistemas que no cuentan con las protecciones adecuadas, lo que teóricamente conduce a la ejecución remota de código en algunas arquitecturas y plataformas.

La posibilidad de que esta vulnerabilidad se explote en la naturaleza es baja debido a la sofisticación de este error de seguridad y al hecho de que una de las condiciones es un certificado malicioso firmado por una CA de confianza.

Al ver que la mayoría de los sistemas y plataformas modernos implementan protecciones integradas para frustrar este tipo de ataques y mitigar estos riesgos, específicamente la ejecución remota de código, el nivel de gravedad se redujo.

Remediación / Referencias

Se recomienda aplicar los parches en su última versión.

Puedes acceder a toda la información en el siguiente enlace:
https://thehackernews.com/2022/11/just-in-openssl-releases-patch-for-2.html

ConnectWise	Vulnerabilidad crítica en ConnectWise Server Backup Solution	PREVENCIÓN

Descripción

La plataforma de software de gestión de servicios de TI ConnectWise ha lanzado parches de software para una vulnerabilidad de seguridad crítica en Recovery R1Soft Server Backup Manager (SBM)

Estado

Se podría abusar del problema, caracterizado como una "neutralización de elementos especiales en la salida utilizados por un componente descendente", para dar como resultado la ejecución de código remoto o la divulgación de información confidencial.
El aviso de ConnectWise señala que la falla afecta a Recover v2.9.7 y anteriores, así como a R1Soft SBM v6.16.3 y anteriores, que se ven afectados por la falla crítica.

En esencia, el problema está relacionado con una vulnerabilidad de omisión de autenticación ascendente en el marco de aplicaciones web Ajax de código abierto de ZK, que se parcheó inicialmente en mayo de 2022.

Los SBM ConnectWise Recover afectados se actualizaron automáticamente a la última versión de Recover (v2.9.9), instando a los clientes a actualizar a SBM v6.16.4 enviado el 28 de octubre de 2022.

Expertos en seguridad identificaron que más de 5,000 instancias de copia de seguridad del administrador del servidor fueron expuestas, lo que podría exponer a las empresas a los riesgos de la cadena de suministro.

Remediación / Referencias

Si bien no hay evidencia de explotación activa de la vulnerabilidad en la naturaleza, una prueba de concepto ideada por los investigadores, muestra que se puede abusar para eludir la autenticación, obtener la ejecución remota de código en SBM y empujar LockBit. 3.0 ransomware a todos los puntos finales posteriores.

Es importante tener en cuenta que la vulnerabilidad ZK ascendente no solo afecta a R1Soft, sino también a cualquier aplicación que utilice una versión sin parches del marco ZK. El acceso que un atacante puede obtener mediante el uso de esta vulnerabilidad de omisión de autenticación es específico de la aplicación que se está explotando; sin embargo, existe un gran potencial para que otras aplicaciones se vean afectadas de manera similar a R1Soft Server Backup Manager.
Por mayor información:
https://thehackernews.com/2022/11/critical-rce-vulnerability-reported-in.html

Conclusiones

Esta nueva edición de noticias vino cargada con varias referentes a la gestión y actualización de vulnerabilidades de software conocido y popular. Para trabajar estos procesos dentro de nuestras organizaciones, son claves algunos elementos y herramientas de gestión operativa, para poder así balancear la economía y los riesgos.

Muchos expertos recomendamos contar con inventario de software y versiones utilizadas en cada uno de nuestros activos más importantes, lo que permitirá evaluar cuándo, dónde y cómo se realizarán actualizaciones de seguridad.

Otra clave son las herramientas de gestión y automatización de estos procesos, ya que los mismos son constantes; mes a mes existen actualizaciones críticas a implementar para así evitar riesgos mayores en las plataformas de sistemas operativos y aplicaciones principales de la operativa.

Cuanto más aceitado y fluido sea este proceso manejado en nuestras organizaciones, acelerará los procesos de cambios tecnológicos, aumentará el cumplimiento y la reducción efectiva de riesgos tecnológicos.

¡Datasec queda a su entera disposición y los invitamos a seguir protegiéndonos!