Boletín de Ciberseguridad

Fecha de Publicación
27/09/2021 - N.º 17

Mes de Setiembre
13/09/2021 - 27/09/2021

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 setiembre se destacan 6 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 1 de fraude activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Google publica fallas que están siendo explotadas actualmente para Chrome

Recientemente fue publicado por Google la versión Chrome 93.0.4577.82, la cual permite solucionar 11 fallos de seguridad, destacando que dos de ellos son ataques de tipo día cero y se ha podido constatar que están siendo explotados actualmente por ciberdelincuentes.

Vulnerabilidad Día Cero en MSHTML y Office

Fuentes oficiales de Microsoft alertan por un error de tipo Zero-Day, que en caso de que un atacante lograra una explotación exitosa, se podría efectuar la ejecución remota de código malicioso en el sistema operativo de los usuarios. También se ha observado que el aprovechamiento de esta vulnerabilidad afecta a los usuarios de Microsoft Office.

Es expuesto Troyano que espía y roba información

Investigadores alertan por un crecimiento sostenido de crímenes vinculados a la comercialización de divisas criptográficas, ya sea mediante la utilización de criptomineros, minería en navegadores o la utilización de ingeniería social para engañar a las víctimas a través de sitios web y aplicaciones fraudulentas.

Se publica lista que reúne las fallas más utilizadas por grupo de Ransomware

Investigadores publican un listado de fallas de seguridad explotados por grupos de ransomware para lograr acceso inicial en los sistemas de sus víctimas. Esta selección engloba un total de 42 vulnerabilidades presentes en 17 tecnologías de distinto tipo.

Google Chrome	**Google publica fallas que están siendo explotadas actualmente para Chrome**	CRÍTICO

Descripción

Recientemente fue publicado por Google la versión Chrome 93.0.4577.82, la cual permite solucionar 11 fallos de seguridad, destacando que dos de ellos son ataques de tipo día cero y se ha podido constatar que están siendo explotados actualmente por ciberdelincuentes.

Esta versión aplica para Windows, Mac y Linux y apunta a corregir estas fallas consideradas como errores de memoria.

Afectados

- Google Chrome.
- Windows.
- Mac.
- Linux.

Estado

Una de estas vulnerabilidades es una escritura fuera de los límites en el motor de JavaScript V8, y el otro error es un error de uso después de la liberación en la API de base de datos indexada.

Aunque estas fallas comúnmente afectan al navegador, los atacantes malintencionados buscan explotarlas mediante la ejecución de código de manera remota y también por escapes de sandbox, entre otras técnicas maliciosas.

"Si bien Google ha revelado que ambos errores se están explotado, no han compartido más información sobre los ataques.

Remediación / Referencias

Recomendamos actualizar las actualizaciones publicadas por el Google.

El proveedor de tecnología ya ha solucionado en 2021, un total de diez fallas de día cero para Google Chrome.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/09/exploits-activos-para-dos-zero-days-en.html
https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html

Office	**Vulnerabilidad Día Cero en MSHTML y Office**	CRÍTICO

Descripción

Fuentes oficiales de Microsoft alertan por un error de tipo Zero-Day, que en caso de que un atacante lograra una explotación exitosa, se podría efectuar la ejecución remota de código malicioso en el sistema operativo de los usuarios. También se ha observado que el aprovechamiento de esta vulnerabilidad afecta a los usuarios de Microsoft Office.

"Diferentes expertos lograron reproducir el ataque en la última versión de Office 2019/Office 365 en equipos con Windows 10 tratándose de un fallo lógico y realmente peligroso."

Esta vulnerabilidad ha sido clasificada con una criticidad de 8.8 sobre 10.

Afectados

- Windows desde la versión 8 a la 10.
- Usuarios de Microsoft Office 2019/Office 365.
- Versiones de Windows Server desde 2008 hasta 2019.

Los usuarios con permisos de administrador son los objetivos apuntados para la implementación de este tipo de ataques.

Estado

La falla de seguridad se encuentra en MSHTML para el navegador de Internet Explorer. Aunque está cada vez más en desuso, este navegador sigue estando presente en muchos de los sistemas operativos actuales y es utilizado para gestionar contenido web. Aplicaciones de Microsoft como Word y PowerPoint dependen de él.

"Los ataques aparecen como controles ActiveX maliciosos incrustados en documentos de Microsoft Office. Estos controles permiten la ejecución de código arbitrario; lo más probable es que los documentos lleguen como archivos adjuntos en mensajes de correo electrónico. Como con cualquier documento adjunto, los atacantes tienen que persuadir a las víctimas para que abran el archivo."

Microsoft Office administra los archivos recibidos a través de la web en vista protegida o mediante la Protección de aplicaciones para Office), dando una prevención para este tipo de ataques. El problema radica en que, si los usuarios hicieran clic en la opción de Habilitar Edición sin tomar en cuenta la procedencia del documento, los mecanismos de seguridad de Microsoft podrían ser vulnerados.

Remediación / Referencias

Microsoft ya publicó la actualización para esa vulnerabilidad:
https://www.catalog.update.microsoft.com/Search.aspx?q=KB5005565

Aunque ya son pocos los que utilizan Internet Explorer, Microsoft recomienda cambiarse a su nuevo navegador, Edge.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/09/zero-day-critico-en-mshtml-e.html9
https://blog.segu-info.com.ar/2021/09/microsoft-publica-el-parche-para-el-0.html

Ransomware en Software ColdFusion

IMPORTANTE

Descripción

Ha sido expuesto un ataque hacia un servidor que contaba con una versión de más de diez años sin actualización para el software ColdFusion 9 de Adobe. Los cibercriminales pudieron tomar el control de forma remota e instalar el ransomware Cring en los dispositivos apuntados.

Los ataques tuvieron origen en una dirección de Internet asignada al ISP ucraniano Green Floid y el servidor vulnerado pertenecía a una empresa de servicios. Este era utilizado para recopilar horarios y datos contables para la nómina, así como para alojar varias máquinas virtuales.

"Los dispositivos que ejecutan software vulnerable y obsoleto son un fruto fácil para los ciberatacantes que buscan una manera fácil de llegar a un objetivo, dijo el investigador principal de Sophos, Andrew Brandt. Lo sorprendente es que este servidor estaba en uso diario activo. A menudo, los dispositivos más vulnerables son máquinas inactivas o fantasmas, ya sea olvidadas o pasadas por alto cuando se trata de parches y actualizaciones".

Afectados

- Windows Server 2008 con software ColdFusion 9 de Adobe.

Estado

Este ransomware cuenta con técnicas sofisticadas para ocultar sus archivos, pudiendo así inyectar código en la memoria, sobrescribiendo los archivos con datos confusos para no dejar rastro alguno.

Los cibercriminales se aprovecharon de una serie de fallos de "Path Traversal" en la consola de administrador en Adobe ColdFusion 9.0.1 y de versiones anteriores que podrían ser vulneradas por ataques remotos para leer archivos arbitrarios, como aquellos que contienen hashes de contraseña de administrador ("password.properties").

"Se cree que el actor malintencionado aprovechó otra vulnerabilidad en ColdFusion, para cargar un archivo de hoja de estilo en cascada (CSS) malicioso en el servidor y, en consecuencia, lo utilizó para cargar un ejecutable de Cobalt Strike Beacon. Este binario, entonces, actuó como un conducto para que los atacantes remotos instalaran payloads adicionales, crearan una cuenta de usuario con privilegios de administrador e incluso deshabilitaran los sistemas de protección y los motores anti-malware como Windows Defender, antes de comenzar el proceso de cifrado."

Remediación / Referencias

Se recomienda a los usuarios con permiso de administrador, no dejar los sistemas comerciales críticos desactualizados.

"Si las organizaciones tienen estos dispositivos en cualquier lugar de su red, pueden estar seguras de que atraerán a los ciberatacantes".

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/09/infeccion-de-ransomware-traves-de-un.html
https://thehackernews.com/2021/09/cring-ransomware-gang-exploits-11-year.html

	**Es expuesto Troyano que espía y roba información**	IMPORTANTE

Descripción

Investigadores alertan por un crecimiento sostenido de crímenes vinculados a la comercialización de divisas criptográficas, ya sea mediante la utilización de criptomineros, minería en navegadores o la utilización de ingeniería social para engañar a las víctimas a través de sitios web y aplicaciones fraudulentas.

En este caso fue detectado un intento de fraude que buscaba suplantar a Safemoon, una criptomoneda creada en marzo de 2021, mediante una aplicación maliciosa que descarga un RAT que espía y roba información

"El termino RAT refiere a herramienta de acceso remoto, pero también es utilizado para referirse a troyanos de acceso remoto. Sucede que es común que los cibercriminales utilicen este tipo de herramientas legítimas para realizar movimiento lateral y/o ejecutar malware, por lo que la diferencia entre un RAT legítimo de uno malicioso está en quienes controlan la herramienta, ya sea una compañía o cibercriminales."

Afectados

- Usuarios que emplean Safemoon para la realización de transacciones comerciales.

Estado

Este intento de fraude utiliza una página web maliciosa basada en la copia de una versión antigua del sitio original. Los enlaces que se encuentran en el sitio falso redirigen al real, pero el engaño radica en el enlace para la descarga de la aplicación que contiene este Troyano.

"Luego de ejecutar el archivo del supuesto instalador de la app, que es un injector bajo el nombre Safemoon-App-v2.0.6.exe, se descargan una serie de archivos, entre ellos el payload de una conocida herramienta de acceso remoto (RAT) llamada Remcos. Es importante destacar que Remcos es un software legítimo que se ofrece en el mercado y que según sus desarrolladores fue pensado originalmente para administrar y monitorear remotamente dispositivos propios. Sin embargo, ya en 2016 autoridades de Estados Unidos hacían referencia a Remcos como un malware, ya que era ampliamente promocionado para su venta en foros de hacking y ha sido utilizado por cibercriminales e incluso grupos de APT en una gran cantidad de campañas maliciosas."

Remediación / Referencias

Recomendamos estar atentos a la confiabilidad y origen de los sitios web con los que se opera y se consultan, así como de las novedades respecto a los engaños e intentos de fraude activos que emplean los atacantes para vulnerar a sus víctimas.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/09/20/vulnerabilidades-mas-utilizadas-grupos-ransomware-obtener-acceso-inicial/

	Actores maliciosos encuentran en Telegram una alternativa para la Deep Web.	PREVENCIÓN

Descripción

Investigaciones recientes explican como Telegram se ha convertido en una opción más por parte de los cibercriminales, para comprar, vender información sensible de sus víctimas, distribuir herramientas de hacking,malwares, exploits para vulnerabilidades nuevas y conocidas, u otro tipo de información

Resulta una novedad esta utilidad negativa que llevan adelante los ciberdelincuentes mediante esta aplicación de mensajería instantánea, ya que históricamente la primera opción era la utilización de la deep web mediante redes anónimas, como la red Onion, para la cual es necesario utilizar el ya conocido navegador Tor.

Afectados

- Usuarios de la aplicación Telegram.

Para enero de 2021, Telegram registraba 500 millones de usuarios activos en todo el mundo. En muchos casos no es solo utilizado de manera personal, ya que muchas de las organizaciones emplean este tipo de tecnología para comercializar y publicitar sus productos y servicios.

Vector de Ataque

"Una investigación reciente realizado por la compañía Cyberint junto a Financial Times reveló que hubo un incremento de más del 100% en el uso de la plataforma de mensajería por parte de cibercriminales. Este incremento se dio en gran medida luego de que WhatsApp anunciara este año los cambios en sus términos y condiciones, lo que llevó a que una gran cantidad de usuarios decidieran migrar a otras aplicaciones de mensajería. Los enlaces hacia grupos de Telegram que fueron compartidos dentro de foros de la dark web pasaron de poco más de 170 mil en 2020 a más de un millón en 2021, afirma el estudio."

Además del aumento de la actividad criminal observada en Telegram, también se ha podido constatar la utilización de la otra aplicación de mensajería instantánea Discord, para alojar malware.

Remediación / Referencias

Las empresas y profesionales de TI deberán estar atentos a la actividad en esta aplicación y a los riesgos que representa la deep web.

En Datasec nuestro destacado equipo de SOC se encuentra en constante desarrollo, adquiriendo las últimas técnicas de vanguardia, para las tareas de monitoreo, seguimiento y análisis de las actividades de las redes de datos, servidores, bases de datos, aplicaciones, sitios web, etc.

La utilización de BeyGoo nos permite tener una visión integral del estado situación de nuestros clientes, garantizando la seguridad y empleando medidas preventivas ante la posibilidad de amenazas futuras.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/09/22/cibercriminales-utilizan-telegram-alternativa-darkweb/#:~:text=seguridad%20de%20ESET.html,Cibercriminales%20utilizan%20cada%20.html.

Se publica lista que reúne las fallas más utilizadas por grupo de Ransomware

PREVENCIÓN

Descripción

Investigadores publican un listado de fallas de seguridad explotados por grupos de ransomware para lograr acceso inicial en los sistemas de sus víctimas. Esta selección engloba un total de 42 vulnerabilidades presentes en 17 tecnologías de distinto tipo.

El aumento de Home – Office debido a la pandemia y la necesidad del uso de soluciones VPN fue utilizado por parte de grupos delictivos para vulnerar a los usuarios.

Afectados

Entre las tecnologías utilizadas para este tipo de ataques estuvieron presentes soluciones VPN:

- Pulse Secure.
- Fortinet.
- Cytrix Hypervisor.
- Citrix Application Delivery Controller.
- Citrix Gateway.
- Microsoft Exchange Server, entre otras.

Vector de Ataque

"Además de intentar abusar del RDP a través de ataques de fuerza bruta o la compra de credenciales de acceso en el mercado clandestino, la explotación de vulnerabilidades es una de las técnicas más utilizadas por las distintas familias de ransomware para lograr acceso en las máquinas de las víctimas y posteriormente a las redes corporativas. Hablamos desde zero days hasta viejas vulnerabilidades reportadas hace algunos años. "

Vulnerabilidades más explotadas:

Remediación / Referencias

Es primordial que las organizaciones lleven a cabo un análisis minucioso de las tecnologías mencionadas en la lista y evaluar la superficie de ataque propia, pudiendo así implementar medidas que permitan minimizar los riesgos de amenazas.

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/09/20/vulnerabilidades-mas-utilizadas-grupos-ransomware-obtener-acceso-inicial/

Conclusiones

Una vez más exhortamos a estar atentos a las noticias publicadas y todo lo referente a la inteligencia de las nuevas amenazas emergentes en la actualidad. Es que, para cada nueva brecha de seguridad que se descubre y más aún si se trata de productos que se utilizan en nuestra organización a nivel de sistemas digitales y demás proveedores de servicios, se debe de estar atentos en la búsqueda de amenazas que puedan venir de diferentes vectores, cómo por ejemplo sucede con las bases de datos públicos de brechas como la de Fortinet (entre otros) que publicamos en esta nueva edición.

A través de los servicios integrales de monitoreo de ciberseguridad (SOC) es que aprovechamos y potenciamos esas capacidades. Contar con un equipo de trabajo orientado y dedicado a estas tareas es cada vez más relevante en cualquier organización humana moderna.

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