



Boletín de Ciberseguridad

Fecha de Publicación
29/03/2021 - N.º 4

Mes de Marzo
15/03/2021 - 29/03/2021

Índice

Introducción	pág. 2
Vulnerabilidades criticas descubiertas en Android y Chrome.....	pág. 3
Errores Críticos en el complemento de Facebook para WordPress.....	pág. 4
Usuarios expuestos en buscador DuckDuckGo.....	pág. 5
Es publicada alerta por vulnerabilidad en routers de Cisco	pág. 6
Equipos ACER atacados por Ransomware REvil	pág. 8
Son detectados equipos infectados por Botnet ZHtrap.....	pág. 10
Preocupación por extensión de Ransomware MountLocker en América Latina.....	pág. 11
Conclusiones.....	pág. 13

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 las 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 marzo se destacan 7 noticias de relevancia: Cuatro sobre vulnerabilidades tecnológicas, una de fraudes activos y dos de prevención.

Aquellas vulnerabilidades de condición crítica a tener recaudo son las siguientes:

Vulnerabilidades críticas descubiertas en Android y Chrome

“Han sido publicadas vulnerabilidades en Google Chrome que permiten que quien realice el exploit, vea cambie o elimine información sensible de los usuarios, a partir de un escalamiento de privilegios.”

Errores Críticos en el complemento de Facebook para WordPress

“Fueron solucionadas dos fallas críticas en el complemento de Facebook para WordPress. Una de estas vulnerabilidades **recibió una puntuación de gravedad CVSS de 9/10.**”



**Vulnerabilidades críticas descubiertas en
Android y Chrome**

CRÍTICO

Descripción

Han sido publicadas vulnerabilidades en Google Chrome que **permiten que quien realice el exploit, vea cambie o elimine información sensible de los usuarios, a partir de un escalamiento de privilegios.**

Mediante un error de uso de memoria después de ser liberada en WebRTC un atacante remoto puede engañar a la víctima para que abra un sitio especialmente diseñado, detonando la falla y permitiendo la ejecución de código malicioso en el sistema.

“WebRTC es un proyecto libre y de código abierto que proporciona a los navegadores web y a las aplicaciones móviles comunicación en tiempo real a través de interfaces de programación de aplicaciones”

En el caso de Android, Google ha informado que se está llevando a cabo un exploit que afecta a los dispositivos que usan prototipos de chips de Qualcomm.

“La falla se refiere a un problema de *“validación de entrada incorrecta”* en el componente de gráficos de Qualcomm que podría explotarse cuando una aplicación diseñada por un atacante solicita acceso a una gran parte de la memoria del dispositivo.”

Afectados

Las versiones afectadas son: Google Chrome, versiones hasta la 89.0.4389.72.
Dispositivos móviles con sistema operativo Android.

Estado

En ambos casos, se trata de vulnerabilidades consideradas "Zero Day" y ya hay indicios de ataques dirigidos sobre estas fallas, aunque no se especifica información sobre los atacantes.

Se destaca que, en el caso de Android para lograr un ataque exitoso el cibercriminal debería tener acceso físico del teléfono de la víctima o acceder por otros medios, por ejemplo, utilizando la técnica de Watering Hole Attack. Una estrategia de ataque que consiste en infectar con malware aquellos sitios web de terceros que sean muy utilizados por los usuarios pertenecientes a la organización. De esta forma cuando los integrantes de la empresa acceden a ese sitio web sus equipos quedan infectados.

Remediación / Referencias

Se deber actualizar el navegador Google Chrome a la versión 89.0.4389.90. La falla de Android ya ha sido parcheada y se espera el lanzamiento de nuevas actualizaciones de seguridad.

Por mayor información al respecto se puede acceder a:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00407-01/>

<https://thehackernews.com/2021/03/warning-new-android-zero-day.html>

<https://blog.segu-info.com.ar/2021/03/explotan-vulnerabilidades-zero-day-en.html>



Errores críticos en el complemento de Facebook para WordPress

CRÍTICO

Descripción

Fueron solucionadas dos fallas críticas en el complemento de Facebook para WordPress. Una de estas vulnerabilidades **recibió una puntuación de gravedad CVSS de 9/10**.

Esta vulnerabilidad permitió que atacantes sin autorización pudieran a acceder a claves privadas de la aplicación. De esta manera **es posible que se pueda llevar a cabo la ejecución remota de código malicioso a través de una debilidad de deserialización**.

La otra vulnerabilidad consiste en una falsificación de solicitudes entre sitios, que conduce a un problema de XSS, se introdujo accidentalmente cuando se cambió el nombre del complemento.

Afectados

Los errores impactan en el plugin de Facebook utilizado para WordPress, anteriormente conocido como Official Facebook Pixel. "El complemento, se utiliza para capturar las acciones de los usuarios cuando visitan una página y para monitorear el tráfico del sitio, se ha instalado en más de 500.000 sitios web."

Estado

No se conoce con exactitud si grupos delictivos están explotando actualmente estas vulnerabilidades, aunque en el caso de éxito, sería considerado crítico.

Se detalla a continuación más especificaciones técnicas en cuanto a la falla más grave:

“La vulnerabilidad, descrita como una inyección de objetos PHP, se encontró en la función `run_action()` del software. Si se genera un *nonce* válido, como mediante el uso de un *script* personalizado, un atacante podría proporcionar al complemento objetos PHP con fines maliciosos e ir tan lejos como para cargar archivos en un sitio web vulnerable y lograr la ejecución remota de código (RCE). ”

Remediación / Referencias

Para poder remediar ambas fallas se han publicado las actualizaciones correspondientes, por lo que se recomienda instalar la última versión disponible del complemento, que actualmente es 3.0.5.

Por mayor información invitamos a acceder a las siguientes referencias:

<https://www.wordfence.com/blog/2021/03/two-vulnerabilities-patched-in-facebook-for-wordpress-plugin/>

<https://blog.segu-info.com.ar/2021/03/vulnerabilidades-criticas-en-facebook.html>



**Usuarios expuestos en el buscador
DuckDuckGo**

IMPORTANTE

Descripción

DuckDuckGo es un buscador de Internet que utiliza la información de sitios de origen público con el objetivo de aumentar los resultados tradicionales y mejorar la relevancia. Se utiliza como una opción alternativa a los buscadores tradicionales.

El objetivo de este navegador es brindar una mayor privacidad en línea, por ejemplo, evitar el seguimiento de rastreadores ocultos, realizar búsquedas privadas y obligar a los sitios a utilizar una conexión cifrada siempre que sea posible. Hay extensiones disponibles para los principales navegadores: Firefox, Chrome y MS Edge.

La extensión de esta herramienta ha presentado fallas que al ser explotadas deja expuesta información de los usuarios. Si se lograra **el cibercriminal podría acceder al historial de búsqueda y a información sensible, como datos personales, direcciones, datos de cuenta bancaria, etc.** Además de afectar el funcionamiento del equipo, pudiendo corromper la visualización de lo que el usuario ve en pantalla.

“Nos encontramos ante un caso de vulnerabilidad uXSS (siglas en inglés de 'universal Cross-Site Scripting'), en la que el atacante es capaz de inyectar código malicioso arbitrario en páginas web visitadas por el usuario usando algún lenguaje de scripting (frecuentemente JavaScript) y explotando vulnerabilidades del lado del cliente. ”

Afectados

Extensión de navegador DuckDuckGoPrivacy Essentials.

Estado

La posibilidad de lograr un ataque exitoso y obtener acceso al equipo de la víctima son escasos, solo podría ser ejecutado por quienes tengan acceso y control sobre el servidor de DuckDuckGo <http://staticcdn.duckduckgo.com>.

“Pero también podría ser aprovechado por su proveedor de alojamiento (nada menos que Microsoft, a través de Azure) o por cualquier atacante que se apodere de dicho servidor (ciberdelincuentes, agencias gubernamentales, etc.).”

Remediación / Referencias

La falla ha sido solucionada con el lanzamiento de la versión 2021.3.8 de la extensión para los tres grandes navegadores. Se aconseja actualizar la herramienta en el gestor de extensiones.

Por mayor información invitamos a acceder a las siguientes referencias:

<https://www.genbeta.com/seguridad/extension-oficial-para-navegadores-duckduckgo-expuso-durante-meses-privacidad-sus-usuarios>

<https://blog.segu-info.com.ar/2021/03/uxss-en-duckduckgo-permitia-espitar.html>



Es publicada alerta por vulnerabilidad en routers de Cisco

IMPORTANTE

Descripción

Se ha puesto en conocimiento una falla de riesgo alto en línea de routers de la empresa tecnológica Cisco. **Si el exploit resultara exitoso un atacante remoto y autenticado ejecutar código o reiniciar aparatos de improviso, resultando en una condición de denegación de servicio (DoS).**

En publicaciones previas se ha puesto de manifiesto fallas en distintos productos que la compañía ha ido solucionando con medidas de remediación directa, con la discontinuidad del producto o un nuevo lanzamiento tecnológico.

Afectados

Productos: Routers RV132W ADSL2+ Wireless-N VPN.

Routers RV134W VDSL2 Wireless-AC VPN.

Estado

La vulnerabilidad nace de una validación inadecuada de la información ingresada por el usuario. Un exploit exitoso podría permitir al atacante ejecutar código arbitrario como usuario raíz en el sistema operativo o hacer que el router se recargue, lo que resultaría en una condición de denegación de servicio (DoS) en el dispositivo afectado. Hasta el momento no se conoce actividad maliciosa explotando esta falla.

Remediación / Referencias

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Por mayor información al respecto se puede acceder a:

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1287>

<https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00409-01/>

**Equipos ACER atacados por Ransomware REvil****IMPORTANTE****Descripción**

El grupo criminal ruso creador del **ransomware REvil** ha **secuestrado información de la empresa Acer, publicándola en la Deep Web, a cambio de la devolución y no divulgación piden la suma de \$50.000.000 USD.**

La amenaza se hizo a través de capturas de pantalla que los atacantes publicaron, mostrando saldos bancarios, hojas de cálculo e información interna de Acer.

Ante la filtración de la noticia la empresa se manifestó indicando lo siguiente:

"Estamos monitoreando nuestros sistemas de TI en busca de cualquier nuevo indicio de conducta anómala. La mejora de nuestros mecanismos de seguridad es continua y queremos asegurarle a nuestros clientes y empleados que este problema no pondrá en riesgo su información sensible".

REvil fue el primer ransomware en generar una nueva técnica de extorsión que consiste en publicar o subastar los datos de las víctimas utilizando la criptomoneda Monero.

Afectados

Acer es una organización que se orienta en crear y ofrecer productos y servicios tecnológicos variados y cuenta con más de 39 000 personas, incluidos distribuidores y personal de servicio técnico, en unos 100 países. **Esto hace que, en el caso de ser vulnerado, podría generarse un riesgo importante de filtración de información de índole privada de sus usuarios.**

Estado

Debido al tipo de código fuente y lo similar que son en sus características, se piensa que podría existir una relación que vincule a los creadores de REvil y GandCrab (ransomware que sigue acaparando el 40 % del mercado). REvil se mantiene funcionando de manera activa y se encuentra en desarrollo constante.

También se manifestó que: "La plataforma de ciberseguridad e inteligencia Advanced Intel detectó que un grupo operador de REvil recientemente estuvo desplegando múltiples ataques contra algunos servidores de Microsoft Exchange"

Métodos que utiliza REvil para conectarse a las víctimas:

ADRecon.

CrackMapExec.

Ghost.

Impacket.

Secretsdump.

Mimikatz.

PentestBox with Metasploit.

Plink.exe.

PowerSploit.

Proxifier.

PsTools (PsExec).

Remediación / Referencias

Aunque la empresa ha sido precavida con sus declaraciones, se cree que hay negociaciones pendientes para la recuperación de la información robada por REvil.

Por mayor información al respecto se puede acceder a:

<https://blog.segu-info.com.ar/2021/03/ransomware-revil-ataca-acer.html>

<https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/>

<https://blog.segu-info.com.ar/2020/11/entrevista-los-creadores-del-ransomware.html>



Son detectados equipos infectados por Botnet ZHtrap

PREVENCIÓN

Descripción

El malware ZHtrap ha sido detectada por un grupo de investigadores de seguridad de 360 Netlab. **Se trata de una botnet que tiene como misión rastrear routers y otros dispositivos de red UPnP infectados y convertirlos en Honeypots.**

“Los honeypots son herramientas de seguridad, y el malware ZHtrap no sólo distingue dispositivos “reales” de aquellos que son “honeypots”, que puede ser más habitual, dado que ningún malware querría ser analizado. ZHtrap también preparará los dispositivos infectados para actuar como honeypots con el objetivo de recopilar información sobre dispositivos previamente infectados por otro malware o controlado por terceros no autorizados, y propagarse empleando dichos dispositivos ya comprometidos.”

Afectados

Se han encontrado tres tipos de variantes, la más completa permite explotar las vulnerabilidades y mantiene una infraestructura de red (es la analizada en el informe de Netlab).

Por ahora las muestras de esta familia no se dirigen a entornos Windows (tampoco lo hacían las muestras iniciales de Mirai).

Vector de Ataque

Se basa en el código fuente de Mirai y es compatible con x86, ARM, MIPS y otras arquitecturas de CPU. Para esto, ZHtrap preparará la máquina víctima, hace una limpieza inicial eliminando procesos y adecuando el equipo. Tras esto, abrirá unos 23 puertos característicos que serán el señuelo para que otros dispositivos se conecten.

“Dentro de las capacidades que tiene este software malicioso podemos mencionar la de llevar a cabo ataques DDoS y hacer un rastreo en busca de nuevos dispositivos vulnerables que pueda infectar. También cuenta con una funcionalidad de puerta trasera que permite descargar y ejecutar cargas útiles maliciosas adicionales.”

Remediación / Referencias

Se exhorta a tomar medidas preventivas y estar atento ante nuevas publicaciones sobre el tema.

Por mayor información al respecto se puede acceder a:

<https://unaaldia.hispasec.com/2021/03/honeypots-del-lado-del-mal-el-reciente-caso-de-zhtrap.html>

<https://blog.segu-info.com.ar/2021/03/zhtrap-malware-convierte-equipos.html>

	<p align="center">Preocupación por extensión de Ransomware MountLocker en América Latina</p>	<p align="center">PREVENCIÓN</p>
---	---	---

Descripción

Este Ransomware, llamado MountLocker (aka AstroTeam) se destaca por robar archivos confidenciales, previamente a ser cifrados en su envío. Luego de concretarse el ataque proceden a pedir una compensación económica a la víctima, mediante extorsión y amenazas de divulgación de dicha información en la Deep Web.

Preocupa su presencia en Latinoamérica ya que este malware se ha ido adaptando y generando nuevas modalidades que le permiten alcanzar de manera directa a las víctimas, evadiendo así las medidas de seguridad implementadas por las organizaciones.

“MountLocker también se une a otras familias de ransomware como Maze (que cerró sus operaciones en noviembre de 2020) que opera un sitio web en la Deep Web para nombrar y avergonzar a las víctimas y proporcionar enlaces a datos filtrados.

Afectados

Uno de los ataques más conocidos previo a su instalación y expansión en nuestro continente, fue en Europa en agosto del 2020. Uno de sus objetivos fue la empresa de seguridad Gunnebo, ubicada en Suecia. El costo del ataque de la publicación fue el robo de 18 gigas de información, de las cuales se especifican documentos confidenciales, incluidos esquemas de bóvedas de bancos de clientes y sistemas de vigilancia.

“La lista de objetivos de cifrado de MountLocker es extensa, con soporte para más de 2.600 extensiones de archivos que abarcan bases de datos, documentos, archivos, imágenes, software de contabilidad, software de seguridad, código fuente, juegos y copias de seguridad.”

Vector de Ataque

MountLocker se caracteriza por ser un tipo de ransomware liviano y eficaz en su ataque. Tras su ejecución, procede a finalizar el software de seguridad, activar el cifrado y crear una nota de rescate, para luego a través de un servicio de chat negociar un precio para la recuperación de la información.

“Utiliza una clave pública RSA-2048 incorporada para cifrar la clave de cifrado, elimina instantáneas de volumen para frustrar la restauración de los archivos cifrados y, finalmente, se elimina del disco para ocultar sus pistas.”

Remediación / Referencias

Se ha observado que este grupo continúa desarrollando y expandiendo sus operaciones delictivas a nivel global, por lo que se exhorta a tomar medidas de recaudo y estar atento a futuras publicaciones.

Por mayor información al respecto se puede acceder a:

<https://thehackernews.com/2020/12/mount-locker-ransomware-offering-double.html>

<https://blog.segu-info.com.ar/2021/03/ransomware-mountlocker-se-extiene-en.html>

Conclusiones

Sobre esta quincena de días, los usuarios de tecnologías de la información deberán estar atentos y ser precavidos, ante los posibles fraudes relacionados a las campañas públicas de vacunación para la prevención de la pandemia originada por Covid-19. Se ha visto la distribución de correos falsos relacionados a campañas que comprometen esta temática de interés general, evitar la apertura de enlaces en estos mails ya que podrían conllevar riesgos.

También es importante seguir trabajando y poniendo foco en los equipos de accesos a teletrabajadores, trabajar la concientización de estos usuarios para evitar que personas remotas puedan abusar del sistema de accesos, muchas veces haciéndose pasar por otras personas de confianza. Reforzar allí los procesos de trabajo es importante, para contar con suficientes medios para comprobar y validar la autenticidad de las personas remotas, por ejemplo, presentando certificados, números, dobles factores de autenticación o hasta se ha vuelto a utilizar la tabla de valores por diccionario, en dónde se cuenta con una matriz precompartida entre las partes y con ello se validan algunos valores que deberían mantenerse secretos.

Las capacitaciones y refuerzos en ayudar a los teletrabajadores a realizar sus funciones, también vino aparejado de recomendaciones de seguridad, es importante que desde tempranos momentos se logren comunicar procesos de trabajo de bajo riesgo y con validaciones de seguridad. En ese sentido próximamente estaremos aportando conocimientos a través de la plataforma educativa de Datasec, en breve tendremos más novedades sobre ello.

Por el lado tecnológico; Existe la campaña de Ransomware MountLocker que se está distribuyendo por América Latina y además de la noticia que publicamos al respecto, es importante tener en consideración que la misma se está haciendo más presente en la zona y que debemos tener los recaudos y respaldos relevantes al día.

Sin más nos despedimos desde el equipo de Datasec les deseamos la mejor protección y el menor riesgo para sus activos.