GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4624

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	2	1	0
MALWARE	0	1	3
NOTICIAS DE CIBERSEGURIDAD	0	1	2

VULNERABILIDADES

Un error crítico de Veeam RCE ahora se utiliza en ataques de ransomware Frag

Recientemente, se ha identificado que el grupo de ransomware Frag está explotando una vulnerabilidad crítica en Veeam Backup & Replication (VBR), conocida como CVE-2024-40711. Esta vulnerabilidad permite a atacantes no autenticados ejecutar código de forma remota en servidores VBR, comprometiendo la integridad de los sistemas de respaldo. Anteriormente, otros grupos de ransomware, como Akira y Fog, también han aprovechado esta misma falla para llevar a cabo sus ataques.

La vulnerabilidad CVE-2024-40711 se origina por una debilidad en la deserialización de datos no confiables, lo que facilita a los atacantes la ejecución de código malicioso en los servidores afectados. Veeam lanzó parches de seguridad el 4 de septiembre de 2024 para mitigar este riesgo. Sin embargo, la explotación de esta falla persiste.

Prioridad: Crítico

Ampliar información:

https://www.bleepingcomputer.com/news/security/critical-veeam-rce-bug-now-used-in-frag-ransomware-attacks/

Palo Alto recomienda proteger la interfaz PAN-OS ante posibles amenazas de RCE

Palo Alto Networks ha emitido una advertencia instando a los usuarios a asegurar la interfaz de gestión de PAN-OS debido a una posible vulnerabilidad de ejecución remota de código (RCE). Aunque los detalles específicos de la vulnerabilidad aún no se conocen, la empresa recomienda configurar la interfaz de gestión según las mejores prácticas y restringir el acceso a direcciones IP internas de confianza para minimizar el riesgo de explotación.

Esta advertencia sigue a la inclusión por parte de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) de una vulnerabilidad crítica previamente parcheada en la herramienta de migración Expedition de Palo Alto Networks. La vulnerabilidad, identificada como CVE-2024-5910, permite la toma de control de cuentas administrativas y el acceso a datos sensibles.

Prioridad: Crítico

Ampliar información:

https://thehackernews.com/2024/11/palo-alto-advises-securing-pan-os.html

---

Cisco lanza parche para la vulnerabilidad crítica URWB en sistemas inalámbricos industriales

Cisco publicó actualizaciones de seguridad para corregir una vulnerabilidad crítica en sus puntos de acceso Ultra-Reliable Wireless Backhaul (URWB). Identificada como CVE-2024-

20418, esta falla permite a atacantes remotos no autenticados ejecutar comandos con privilegios de root en el sistema operativo subyacente de los dispositivos afectados. La vulnerabilidad se origina por una falta de validación de entradas en la interfaz de gestión web del software Cisco Unified Industrial Wireless.

Los productos impactados incluyen los puntos de acceso Catalyst IW9165D Heavy Duty, Catalyst IW9165E Rugged y Catalyst IW9167E Heavy Duty, siempre que estén operando en modo URWB. Cisco ha lanzado la versión 17.15.1 de su software para abordar este problema y recomienda a los usuarios que utilicen versiones 17.14 o anteriores que actualicen a la versión corregida. Aunque no hay evidencia de explotación activa de esta vulnerabilidad, es esencial que los usuarios apliquen las actualizaciones correspondientes para proteger sus sistemas contra posibles amenazas.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/cisco-releases-patch-for-critical-urwb.html

---

Recomendaciones generales sobre vulnerabilidades:

Para reducir las vulnerabilidades en los sistemas, se sugieren las siguientes acciones clave:

Aplicar parches de seguridad de forma regular para solucionar fallos conocidos.

Añadir una capa adicional de seguridad, como la autenticación de dos factores (2FA), para complicar el acceso no autorizado.

Restringir los permisos de usuarios y aplicaciones, limitando el acceso solo a lo necesario para reducir riesgos.

Utilizar herramientas de detección de intrusiones para monitorizar y detectar comportamientos sospechosos.

Estas medidas son esenciales para contribuir a fortalecer la seguridad de los sistemas.

MALWARE

El nuevo malware CRON#TRAP infecta Windows ocultándose en una máquina virtual Linux

Investigadores de ciberseguridad han identificado una nueva campaña de malware denominada CRON#TRAP, que compromete sistemas Windows mediante la ejecución de una máquina virtual Linux para evadir la detección por parte de soluciones antivirus tradicionales. El ataque se inicia con un archivo malicioso de acceso directo (LNK) distribuido, presumiblemente, a través de correos electrónicos de phishing. Al ejecutarse, este archivo despliega un entorno Linux ligero utilizando QEMU, un emulador de código abierto, que contiene un backdoor preconfigurado. Este backdoor establece una conexión automática con un servidor de comando y control (C2), otorgando a los atacantes acceso remoto al sistema comprometido.

La táctica de CRON#TRAP y su capacidad de ocultar las actividades maliciosas, dificulta su detección por herramientas de seguridad convencionales. Este enfoque permite a los atacantes mantener una presencia persistente y discreta en los sistemas afectados, facilitando la ejecución de actividades maliciosas adicionales sin ser detectados. La sofisticación de esta técnica subraya la necesidad de que las organizaciones implementen medidas de seguridad avanzadas y actualicen regularmente sus sistemas para protegerse contra amenazas emergentes.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/new-crontrap-malware-infects-windows-by.html

Cibercriminales utilizan un exploit de Excel para propagar el malware Remcos RAT sin archivos

Los cibercriminales han lanzado una campaña de phishing que distribuye una variante sin archivos del malware Remcos RAT mediante una vulnerabilidad en archivos de Excel. Los atacantes envían correos electrónicos que tratan de órdenes de compra que incitan a las víctimas a abrir un archivo de Excel malicioso, el cual explota la vulnerabilidad CVE-2017-0199 (ejecución de código remoto en Office) para ejecutar código de manera remota. Cuando las víctimas abren el archivo de Excel, se inicia un proceso que permite descargar y ejecutar un archivo de aplicación HTML (HTA) desde un servidor remoto utilizando mshta.exe.

Una vez ejecutado el archivo HTA, se ejecuta un script que descarga un programa binario, el cual lanza un segundo comando de PowerShell ofuscado. Esta técnica permite cargar Remcos RAT directamente en la memoria del sistema, evitando que se cree un archivo en el disco, lo que convierte el ataque en "fileless" o sin archivos permanentes. Remcos RAT proporciona a los atacantes acceso remoto al sistema, permitiendo recolectar datos sensibles, ejecutar comandos, gestionar procesos y activar dispositivos como la cámara y el micrófono de la víctima.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/cybercriminals-use-excel-exploit-to.html

---

El malware AndroxGh0st integra la botnet Mozi para atacar servicios de IoT y de la nube

Investigadores de CloudSEK han identificado que el malware AndroxGh0st ha ampliado su alcance al integrar funcionalidades del botnet Mozi, enfocándose en dispositivos IoT y servicios en la nube. AndroxGh0st, conocido por atacar aplicaciones Laravel para extraer

credenciales de servicios como AWS, SendGrid y Twilio, ahora explota una variedad de vulnerabilidades, incluyendo CVE-2014-2120, CVE-2018-10561, CVE-2018-10562, CVE-2021-26086, CVE-2021-41277, CVE-2022-1040, CVE-2022-21587, CVE-2023-1389, CVE-2024-4577 y CVE-2024-36401, para comprometer infraestructuras críticas.

La integración de Mozi, un botnet previamente desmantelado en 2021, permite a AndroxGh0st utilizar métodos de ejecución remota de código y robo de credenciales para mantener acceso persistente a sistemas comprometidos. Esta evolución representa una amenaza significativa para la seguridad de dispositivos IoT y servicios en la nube, destacando la necesidad de aplicar parches de seguridad y seguir las mejores prácticas de ciberseguridad para mitigar riesgos asociados con estas vulnerabilidades.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/androxgh0st-malware-integrates-mozi.html

---

Paquetes NPM maliciosos atacan a usuarios de Roblox con malware

Recientemente, se ha detectado una campaña maliciosa que introduce paquetes comprometidos en el repositorio de Node Package Manager (NPM), dirigidos específicamente a desarrolladores de Roblox. Estos paquetes, como node-dlls, ro.dll, autoadv y rolimons-api, contienen código ofuscado diseñado para descargar y ejecutar malware de tipo stealer, como Skuld y Blank Grabber. Este software malicioso, escrito en Go y Python, tiene la capacidad de recopilar información sensible de los sistemas infectados y transmitirla a través de canales como Discord y Telegram.

La estrategia de los atacantes incluye la suplantación de paquetes legítimos mediante técnicas de typosquatting, aprovechando la confianza de los desarrolladores en nombres familiares. Así, node-dlls imita al paquete legítimo node-dll, y rolimons-api imita la API de Rolimon's.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/malicious-npm-packages-target-roblox.html

---

Recomendaciones generales sobre malware:

Para protegerse del malware, es fundamental:

Mantener el software y los sistemas operativos actualizados de manera regular, ya que los atacantes suelen aprovechar vulnerabilidades en versiones obsoletas.

Utilizar programas antivirus y antimalware confiables, asegurándose de que siempre estén actualizados.

Activar la autenticación multifactor (MFA) para asegurar cuentas sensibles y dificultar el acceso no autorizado.

Ser cauteloso con correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de infección por malware.

Hacer copias de seguridad periódicas de los archivos importantes, para evitar pérdidas en caso de ataques como el ransomware.

Restringir los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Paquete malicioso PyPI con 37.000 descargas roba claves de AWS

Investigadores de seguridad han descubierto un paquete malicioso en el repositorio de Python Package Index (PyPI) llamado “fabrice”, que ha estado activo desde 2021 y ha sido

descargado más de 37,000 veces. Este paquete se hace pasar por "fabric", una biblioteca legítima utilizada para ejecutar comandos remotos a través de SSH, aprovechando la similitud en los nombres para engañar a los desarrolladores. Una vez instalado, "fabrice" ejecuta scripts específicos según el sistema operativo: en Linux, crea un directorio oculto y descarga scripts shell codificados; en Windows, descarga y ejecuta un archivo malicioso. El objetivo principal de este paquete es robar credenciales de Amazon Web Services (AWS) utilizando la biblioteca Boto3 para acceder y exfiltrar las claves de acceso y secretas de AWS a un servidor controlado por los atacantes.

Prioridad: Urgente

Ampliar información:

https://www.bleepingcomputer.com/news/security/malicious-pypi-package-with-37-000-downloads-steals-aws-keys/

Canadá ordena a TikTok cerrar operaciones en Canadá por problemas de seguridad

El gobierno canadiense ordenó a TikTok Technology Canada Inc., filial de ByteDance Ltd., cesar sus operaciones en el país debido a preocupaciones de seguridad nacional. Esta decisión se basa en una revisión exhaustiva realizada por las agencias de seguridad e inteligencia de Canadá, que identificaron riesgos específicos asociados con las actividades de ByteDance en territorio canadiense.

A pesar de esta medida, el gobierno no restringirá el acceso de los ciudadanos canadienses a la aplicación TikTok ni limitará su capacidad para crear contenido en la plataforma. Sin embargo, se insta a los usuarios a adoptar prácticas de ciberseguridad responsables y a evaluar los posibles riesgos relacionados con el uso de aplicaciones de redes sociales, especialmente en lo que respecta al manejo de su información personal.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/canada-orders-tiktok-to-shut-down.html

---

Hackers utilizan la concatenación de archivos ZIP para evadir la detección

Los ciberdelincuentes han adoptado una técnica denominada "concatenación de archivos ZIP" para evadir la detección de soluciones de seguridad. Esta estrategia implica combinar múltiples archivos ZIP en uno solo, aprovechando las diferencias en cómo los gestores de archivos y los analizadores de seguridad procesan estos archivos concatenados. Al hacerlo, los atacantes pueden ocultar cargas maliciosas dentro de archivos comprimidos que parecen inofensivos, dificultando su identificación por parte de los sistemas de seguridad.

La técnica se basa en crear varios archivos ZIP, donde uno contiene el malware y los demás archivos benignos. Estos archivos se unen en un solo archivo concatenado. Al abrir el archivo, algunos gestores de archivos pueden mostrar solo el contenido benigno, mientras que otros pueden acceder al contenido malicioso. Esta variabilidad en la interpretación de los archivos ZIP concatenados permite a los atacantes distribuir malware de manera más efectiva, eludiendo las medidas de seguridad tradicionales.

Prioridad: Importante

Ampliar información:

https://www.bleepingcomputer.com/news/security/hackers-now-use-zip-file-concatenation-to-evade-detection/