GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4724

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	2
NOTICIAS DE CIBERSEGURIDAD	0	1	2

VULNERABILIDADES

Falla en PostgreSQL permite a los piratas informáticos explotar las variables del entorno

Investigadores de ciberseguridad han identificado una vulnerabilidad en PostgreSQL, el sistema de base de datos de código abierto, que permite a usuarios sin privilegios modificar variables de entorno, lo que podría derivar en la ejecución de código arbitrario o la divulgación de información. Esta vulnerabilidad, catalogada como CVE-2024-10979, afecta a las versiones anteriores a 17.1, 16.5, 15.9, 14.14, 13.17 y 12.21 de PostgreSQL.

La falla reside en el control inadecuado de variables de entorno en PostgreSQL PL/Perl, permitiendo que un usuario sin privilegios altere variables sensibles del proceso, como PATH. Esto puede facilitar la ejecución de código arbitrario, incluso sin acceso al sistema operativo del servidor de la base de datos. Se recomienda a los usuarios actualizar a las

versiones corregidas y restringir las extensiones permitidas, limitando los permisos de creación de funciones según el principio de privilegios mínimos.

Prioridad: Crítico

Ampliar información:

https://thehackernews.com/2024/11/high-severity-flaw-in-postgresql-allows.html

---

CISA detecta dos vulnerabilidades de seguridad explotadas activamente en Palo Alto; se confirma un nuevo ataque RCE

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha alertado sobre la explotación activa de dos vulnerabilidades críticas en el software Expedition de Palo Alto Networks. Estas fallas, identificadas como CVE-2024-9463 y CVE-2024-9465, permiten a atacantes no autenticados ejecutar comandos del sistema operativo con privilegios de root o acceder a contenidos de la base de datos, lo que podría exponer información sensible como nombres de usuario, contraseñas en texto claro y configuraciones de dispositivos.

Palo Alto Networks abordó estas vulnerabilidades en actualizaciones de seguridad publicadas el 9 de octubre de 2024. Sin embargo, CISA ha instado a las agencias federales a aplicar las actualizaciones necesarias antes del 5 de diciembre de 2024, debido a la evidencia de explotación activa. Además, la empresa ha reconocido informes sobre la explotación de una nueva vulnerabilidad de ejecución remota de comandos en interfaces de gestión de firewalls expuestas a internet.

Prioridad: Crítico

Ampliar información:

https://thehackernews.com/2024/11/cisa-flags-critical-palo-alto-network.html

---

Nuevas fallas en Citrix Virtual Apps permiten ataques RCE a través de una configuración incorrecta de MSMQ

Investigadores de ciberseguridad han descubierto vulnerabilidades en Citrix Virtual Apps and Desktops que podrían permitir la ejecución remota de código sin autenticación. Estas fallas, identificadas como CVE-2024-8068 (escalada de privilegios para acceder a la cuenta de NetworkService) y CVE-2024-8069 (ejecución remota de código limitada con el privilegio de acceso a una cuenta de servicio de red), están relacionadas con la configuración incorrecta de Microsoft Message Queuing (MSMQ) y el uso inseguro de la clase BinaryFormatter en el componente de grabación de sesiones. Citrix ha abordado estas vulnerabilidades en las versiones actualizadas de su software.

La explotación exitosa de estas vulnerabilidades requiere que el atacante sea un usuario autenticado en el mismo dominio del Directorio Activo y en la misma intranet que el servidor de grabación de sesiones. Se recomienda a los administradores actualizar a las versiones corregidas y revisar las configuraciones de seguridad para mitigar posibles riesgos.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/new-flaws-in-citrix-virtual-apps-enable.html

---

Recomendaciones generales sobre vulnerabilidades:

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

Implementar configuraciones de seguridad adecuadas, asegurándose de deshabilitar servicios y puertos innecesarios para minimizar superficies de ataque.

Realizar auditorías periódicas de seguridad para identificar vulnerabilidades y corregirlas antes de que puedan ser explotadas.

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

Actualizar y reforzar las políticas de contraseñas, promoviendo el uso de contraseñas únicas y complejas junto con gestores de contraseñas.

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 RustyAttr ataca macOS mediante el abuso de atributos extendidos

Expertos han detectado una nueva amenaza dirigida a sistemas macOS denominada RustyAttr. Este software malicioso explota los atributos extendidos de los archivos en macOS para ofuscar y ejecutar código dañino sin ser identificado. Su distribución ocurre mediante aplicaciones desarrolladas con el framework Tauri y firmadas con certificados robados, facilitando su instalación en los equipos afectados.

Al activarse, RustyAttr despliega un sitio web falso que ejecuta un script malicioso, diseñado para extraer y activar contenido oculto en los atributos extendidos del archivo. Aunque aún no se han identificado objetivos claros ni cargas útiles adicionales, se cree que esta técnica podría estar relacionada con el grupo Lazarus, conocido por operaciones avanzadas de ciberespionaje. Para mitigar riesgos, se aconseja a los usuarios de macOS mantener Gatekeeper habilitado y evitar instalar software de fuentes no confiables.

Prioridad: Urgente

Ampliar información:

https://thehackernews.com/2024/11/new-rustyattr-malware-targets-macos.html

---

Hackers iraníes utilizan el señuelo del "Dream Job" para desplegar el malware SnailResin en ataques aeroespaciales

El grupo de ciberamenazas iraní TA455 ha implementado tácticas similares a las del grupo norcoreano Lazarus, utilizando ofertas de trabajo falsas para atacar a la industria aeroespacial desde septiembre de 2023. Esta campaña distribuye el malware SnailResin, que activa el backdoor SlugResin, permitiendo a los atacantes acceder remotamente a sistemas comprometidos.

TA455, también conocido como UNC1549 y Yellow Dev 13, forma parte del grupo APT35, vinculado al Cuerpo de la Guardia Revolucionaria Islámica de Irán. Los atacantes emplean sitios web de reclutamiento falsos y perfiles de LinkedIn para distribuir archivos ZIP maliciosos que contienen ejecutables y DLL diseñados para cargar el malware. Se recomienda a las organizaciones del sector aeroespacial reforzar sus medidas de seguridad y educar a su personal sobre tácticas de ingeniería social para mitigar estos riesgos.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/iranian-hackers-use-dream-job-lures-to.html

---

Grupo de hackers vietnamita despliega un nuevo Stealer de PXA dirigido a Europa y Asia

Un grupo de ciberdelincuentes vietnamita ha lanzado una campaña dirigida a entidades gubernamentales y educativas en Europa y Asia, utilizando un nuevo malware basado en Python denominado PXA Stealer. Este software malicioso está diseñado para extraer información sensible, incluyendo credenciales de cuentas en línea, datos financieros, cookies de navegadores y detalles de software de juegos. Una característica destacada de PXA Stealer es su capacidad para descifrar la contraseña maestra del navegador de la víctima, facilitando el acceso a credenciales almacenadas.

La distribución de PXA Stealer se realiza a través de correos electrónicos de phishing que contienen archivos adjuntos en formato ZIP. Estos archivos incluyen un cargador desarrollado en Rust y scripts por lotes que, al ejecutarse, descargan y ejecutan el malware, además de deshabilitar programas antivirus en el sistema afectado. El malware muestra un interés particular en las cookies de Facebook, utilizando estas para interactuar con Facebook Ads Manager y la API Graph, con el objetivo de recopilar información adicional sobre las cuentas comprometidas y sus actividades publicitarias.

Prioridad: Importante

Ampliar información:

https://thehackernews.com/2024/11/vietnamese-hacker-group-deploys-new-pxa.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

NSO Group utilizó otro día cero de WhatsApp después de ser demandado

Según documentos judiciales recientes, la empresa israelí de vigilancia NSO Group utilizó múltiples exploits de día cero en WhatsApp, incluyendo uno denominado "Erised", para desplegar su spyware Pegasus en ataques sin interacción del usuario. Estas acciones ocurrieron incluso después de que WhatsApp demandará a NSO Group en 2019 por presuntas actividades de espionaje.

El exploit "Erised" permitía a NSO Group instalar Pegasus en dispositivos de las víctimas sin necesidad de que estas realizaran alguna acción, aprovechando vulnerabilidades no conocidas en WhatsApp. Este spyware otorgaba acceso completo a los dispositivos comprometidos, permitiendo la vigilancia de comunicaciones y actividades.

Prioridad: Urgente

Ampliar información:

https://www.bleepingcomputer.com/news/security/nso-group-used-another-whatsapp-zero-day-after-being-sued-court-docs-say/

T-Mobile confirma que fue víctima de un ataque informático

T-Mobile ha confirmado que fue víctima de un ciberataque en una reciente ola de brechas de seguridad que afectaron a varias empresas de telecomunicaciones. Según la compañía, no se han detectado impactos significativos en sus sistemas ni evidencia de que la información de los clientes haya sido comprometida. Este incidente se enmarca en una serie de ataques atribuidos al grupo de amenazas persistentes avanzadas conocido como Salt Typhoon, vinculado a agencias de inteligencia chinas.

Salt Typhoon ha llevado a cabo campañas de espionaje cibernético dirigidas a múltiples empresas de telecomunicaciones en Estados Unidos, incluyendo AT&T, Verizon y Lumen Technologies. Estos ataques buscan acceder a comunicaciones privadas, registros de llamadas y solicitudes de información de las fuerzas del orden. T-Mobile continúa monitoreando de cerca la situación, colaborando con sus pares en la industria y las autoridades pertinentes para mitigar cualquier riesgo potencial.

Prioridad: Importante

Ampliar información:

https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/

Microsoft retira actualizaciones de seguridad de Exchange por problemas con la entrega de correo

Microsoft ha retirado las actualizaciones de seguridad de Exchange Server publicadas en noviembre de 2024 debido a problemas en la entrega de correos electrónicos en servidores que utilizan reglas de flujo de correo personalizadas. Administradores reportaron que, tras instalar estas actualizaciones, el flujo de correos se detenía por completo, afectando a

organizaciones que emplean reglas de transporte o políticas de prevención de pérdida de datos (DLP).

La compañía ha pausado la distribución de estas actualizaciones a través de Windows Update y el Centro de Descargas mientras investiga el problema. Se recomienda a los administradores que experimenten interrupciones en el flujo de correo desinstalar las actualizaciones problemáticas hasta que se publique una solución definitiva. Aquellos que no utilicen reglas de flujo de correo pueden optar por mantener las actualizaciones, ya que no se han reportado problemas en esos casos.

Prioridad: Importante

Ampliar información:

https://www.bleepingcomputer.com/news/microsoft/microsoft-pulls-exchange-security-updates-over-mail-delivery-issues/