GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0425

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por expertos de 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	1	3	1
MALWARE	0	3	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

Descubren vulnerabilidad crítica en el marco Llama-stack de Meta

El equipo de investigación Oligo reveló una vulnerabilidad crítica (CVE-2024-50050) en el marco Llama-stack de Meta, que permite a atacantes remotos ejecutar código arbitrario en servidores afectados.

Este fallo, calificado con un CVSS de 9.8, se originó en el método recv_pyobj, que utiliza el módulo inseguro Pickle para deserializar datos. Meta lanzó un parche en octubre de 2024 (versión 0.0.41), reemplazando Pickle por JSON y Pydantic para mayor seguridad. Se insta a los usuarios a actualizar el marco reforzando las prácticas de seguridad en sus implementaciones.

Prioridad: **Importante**

Ampliar información:

https://gbhackers.com/critical-vulnerability-in-meta-llama-framework/

Vulnerabilidad RCE de "clic cero" en Outlook (CVE-2025-21298)

Microsoft emitió un parche crítico para abordar CVE-2025-21298, una vulnerabilidad de ejecución remota de código (RCE) en la biblioteca ole32.dll de Windows. Este fallo, que explota un error de doble liberación de memoria, puede activarse simplemente al previsualizar un archivo RTF malicioso en Microsoft Outlook, sin interacción del usuario. El PoC ya publicado aumenta el riesgo de ataques, afectando a sistemas desde Windows Server 2008 hasta Server 2025 y Windows 10/11.

Microsoft corrigió el problema en su actualización de enero de 2025 y recomienda instalar el parche, deshabilitar vistas previas de RTF, reforzando la seguridad del correo electrónico.

Prioridad: **Urgente**

Ampliar información:

https://gbhackers.com/zero-click-outlook-rce-vulnerability/

Descubren vulnerabilidad de inyección SQL en DevBlogs de Microsoft

Un investigador de seguridad identificó una vulnerabilidad crítica de inyección SQL en el subdominio DevBlogs de Microsoft (https://devblogs.microsoft.com), que permite a atacantes manipular la base de datos subyacente mediante consultas

maliciosas. El fallo, localizado en el endpoint admin-ajax.php del CMS WordPress, fue explotado exitosamente para extraer nombres de bases de datos utilizando herramientas como sqlmap.

A pesar de su gravedad, Microsoft consideró el subdominio "fuera de alcance" en su programa de recompensas, dejando el problema sin resolver al momento. Se destaca la necesidad de validar entradas y auditar regularmente la seguridad en plataformas públicas.

Prioridad: Crítico

Ampliar información:

https://gbhackers.com/sql-injection-vulnerability-in-microsofts-devblogs/

Cisco corrige tres vulnerabilidades críticas, incluyendo fallos en Meeting Management y ClamAV

Cisco ha lanzado parches para tres vulnerabilidades, entre ellas la crítica CVE-2025-20156 (puntaje CVSS 9.9) en el API REST de Meeting Management, que permite a atacantes remotos elevar privilegios a nivel de administrador mediante solicitudes API. No existen soluciones temporales y los usuarios deben actualizar a la versión 3.9.1 o posterior. Otro fallo, CVE-2025-20165, afecta el subsistema SIP de BroadWorks, permitiendo ataques de denegación de servicio (DoS) al enviar solicitudes SIP masivas. Fue corregido en BroadWorks RI.2024.11.

Finalmente, CVE-2025-20128, un problema de desbordamiento de búfer en ClamAV, podría causar la interrupción del proceso de análisis al escanear archivos manipulados. Aunque existe código de prueba (PoC), no hay evidencia de

explotación activa. Cisco insta a aplicar los parches disponibles para mitigar estos riesgos.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/cisco-patches-critical-vulnerability-in-meeting-management

---

Vulnerabilidades en Git expusieron credenciales de usuarios

El protocolo de recuperación de credenciales de Git presentó vulnerabilidades que permitían a atacantes filtrar credenciales de usuarios, según informó el investigador RyotaK. Los problemas, como el CVE-2025-23040 y CVE-2024-53263, se originaron en el manejo inadecuado de caracteres de retorno de carro en URLs manipuladas. Esto afectó herramientas como GitHub Desktop, Git LFS y Git Credential Manager, posibilitando el acceso indebido a credenciales almacenadas.

Git lanzó parches en la versión 2.48.1 y actualizaciones para GitHub Desktop (3.4.12), Git LFS (3.6.1) y Git Credential Manager (2.6.1) para mitigar estos problemas. Las soluciones incluyen validaciones más estrictas para evitar la explotación de URLs maliciosas y evitar el filtrado de credenciales entre servidores.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/git-vulnerabilities-led-to-credentials-exposure/

Recomendaciones generales sobre vulnerabilidades:

- Aplique siempre los parches de seguridad más recientes proporcionados por los fabricantes para corregir vulnerabilidades críticas y mitigar riesgos de explotación.
- Implemente sistemas de monitoreo para detectar actividades sospechosas, como accesos no autorizados o cambios no autorizados en configuraciones críticas.
- Configure alertas para comportamientos anómalos que puedan indicar la explotación de vulnerabilidades.
- Aplique controles de acceso basados en roles (RBAC) y realice segmentación de red para limitar el impacto en caso de que una vulnerabilidad sea explotada en un sistema.
- Limite el acceso a servicios no utilizados, cierre puertos innecesarios y restrinja el acceso solo a usuarios o redes confiables para reducir la exposición a ataques.
- Realice pruebas de penetración y auditorías de seguridad periódicas para identificar vulnerabilidades no reportadas o posibles brechas en la infraestructura.

MALWARE

Campaña maliciosa redirige a usuarios de macOS a un sitio falso de Homebrew con malware

Una campaña de malvertising ha estado apuntando a usuarios de macOS mediante anuncios de Google que redirigen a un sitio falso de Homebrew (‘brewe.sh’). Este sitio imitaba al legítimo (‘brew.sh’) y contenía un comando cURL que instalaba el malware Amos Stealer. Este software malicioso, conocido desde

2023, roba contraseñas, datos del Keychain, información del sistema, cookies, billeteras de criptomonedas y más. Google eliminó los anuncios maliciosos, del mismo modo, suspendió las cuentas de los anunciantes implicados, aunque aún investiga cómo lograron evadir sus sistemas de detección.

Se insta a los usuarios a reportar anuncios fraudulentos y verificar cuidadosamente los enlaces antes de ejecutar comandos.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/homebrew-macos-users-targeted-with-information-stealer-malware/

Grupos de ransomware abusan de la plataforma Office 365 para acceder a organizaciones

Investigadores de Sophos identificaron dos grupos de ransomware, STAC5143 y STAC5777, que están explotando servicios de Microsoft 365, con configuraciones predeterminadas para atacar a usuarios internos de empresas.

Los dos grupos utilizan sus propios inquilinos de Microsoft 365 y aprovechan una configuración predeterminada de Teams que permite a los usuarios externos contactar a los usuarios internos. STAC5143 emplea capacidades remotas de Teams y herramientas basadas en Java, mientras que STAC5777 utiliza Microsoft Quick Assist y cambios manuales en la configuración para desplegar malware. Ambos grupos emplean tácticas como correos electrónicos de spam, suplantación

de soporte técnico, así como el uso de herramientas remotas de Microsoft para instalar malware y mover lateralmente por las redes comprometidas.

Prioridad: Urgente

Ampliar información:

https://securityaffairs.com/173328/cyber-crime/ransomware-groups-abuse-microsofts-office-365-platform.html

---

Ataques de ransomware a ESXi usan túneles SSH para evitar detección

Investigadores de Sygnia alertan sobre los ataques de ransomware a entornos virtualizados, en los que los atacantes emplean túneles SSH para evitar ser detectados. Los grupos de ransomware explotan dispositivos ESXi no monitoreados para acceder y persistir en redes corporativas, utilizando técnicas como SSH para crear túneles SOCKS no detectados para la comunicación con los servidores de comando o control (C2).

Los atacantes acceden a los dispositivos comprometiendo credenciales administrativas o aprovechando vulnerabilidades conocidas para eludir la autenticación. Una vez dentro, configuran el túnel utilizando SSH o herramientas comunes similares. La capacidad de ESXi para dividir los registros en múltiples archivos complica las investigaciones forenses, por lo que se recomienda configurar el reenvío de registros para centralizar el monitoreo y facilitar la detección de actividades maliciosas.

Prioridad: Urgente

Ampliar información:

https://securityaffairs.com/173487/cyber-crime/esxi-ransomware-attacks-use-ssh-tunnels-to-avoid-detection.html

---

Recomendaciones generales sobre malware:

- Asegúrese de que los sistemas de detección de amenazas y antivirus estén actualizados para detectar malware conocido y prevenir ataques.
- No descargue software ni abra enlaces de correos electrónicos o sitios web desconocidos. Fomente el uso exclusivo de repositorios oficiales para minimizar el riesgo de infecciones.
- Eduque a los empleados y usuarios sobre cómo identificar intentos de phishing y engaños en línea, ya que muchos ataques de malware se inician a través de técnicas de ingeniería social.
- Limite los privilegios de usuario y evite que los empleados instalen o ejecuten software no autorizado en sus sistemas corporativos para reducir la superficie de ataque.
- Monitoree el tráfico de red de manera continua para detectar actividades sospechosas, como conexiones a servidores remotos desconocidos, lo que podría indicar que un sistema ha sido comprometido.

NOTICIAS DE CIBERSEGURIDAD

Riesgos de la clonación de voz y medidas para prevenir estafas

El avance de la inteligencia artificial ha facilitado la clonación de voz, permitiendo a estafadores imitar voces con solo unos segundos de grabación, lo que ha resultado en fraudes significativos, como falsos secuestros y suplantación de

autoridades. Los ciberdelincuentes obtienen muestras de plataformas como YouTube o TikTok para crear audios falsos que engañan a las víctimas.

Casos recientes incluyen un robo de 51 millones de dólares en Emiratos Árabes y estafas en EE. UU. y Australia. Para prevenir estas amenazas, se recomiendan campañas de concienciación, autenticación biométrica, autenticación multifactor o regulaciones actualizadas para mitigar los riesgos asociados.

Prioridad: Importante

Ampliar información:

https://www.pandasecurity.com/es/mediacenter/los-riesgos-de-la-clonacion-de-voz-y-como-prevenir-este-tipo-de-estafas/