GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0725

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
VULNERABIILIDADES	2	1	0
MALWARE	0	2	0
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Vulnerabilidad en PAN-OS permite omisión de autenticación en firewalls de Palo Alto Networks

Recientemente, se ha detectado que actores malintencionados están aprovechando una vulnerabilidad en el software PAN-OS de los firewalls de Palo Alto Networks. Esta falla, identificada como CVE-2025-0108, permite a atacantes no autenticados eludir los mecanismos de autenticación en la interfaz web de administración de PAN-OS, otorgándoles la capacidad de invocar ciertos scripts PHP y comprometer la integridad y confidencialidad del sistema. La vulnerabilidad afecta a las versiones 10.1.14-h9, 10.2.13-h3, 11.1.6-h1 y 11.2.4-h4 de PAN-OS. Es importante destacar que la versión 11.0 también es vulnerable; sin embargo, al haber alcanzado su fin de vida útil, no recibirá actualizaciones de seguridad.

Para mitigar este riesgo, Palo Alto Networks ha incitado a los administradores a actualizar sus firewalls a las versiones corregidas mencionadas anteriormente. Además, se recomienda restringir el acceso a la interfaz de administración web únicamente a redes de confianza y deshabilitar el acceso desde redes públicas o redes no seguras. Estas medidas ayudarán a prevenir posibles intentos de explotación de la vulnerabilidad y a mantener la seguridad de los sistemas protegidos por los firewalls de Palo Alto Networks.

Prioridad: Crítico.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/hackers-exploit-authentication-bypass-in-palo-alto-networks-pan-os/

Vulnerabilidad en PostgreSQL explotada junto con Zero-Day de BeyondTrust en ataques dirigidos

Se ha descubierto que los actores responsables de explotar una vulnerabilidad de Zero-Day en los productos BeyondTrust Privileged Remote Access (PRA) y Remote Support (RS) en diciembre de 2024 también aprovecharon una falla previamente desconocida en PostgreSQL. Esta vulnerabilidad, identificada como CVE-2025-1094 con una puntuación CVSS de 8.1, afecta la herramienta interactiva psql de PostgreSQL. Esta permite a un atacante, mediante una inyección SQL, ejecutar comandos arbitrarios al aprovechar la capacidad de psql para ejecutar meta-comandos.

La vulnerabilidad se origina en la forma en que PostgreSQL maneja caracteres UTF-8 inválidos, lo que abre la posibilidad de que un atacante ejecute comandos de shell a través de una inyección SQL utilizando el comando abreviado "!". PostgreSQL ha lanzado actualizaciones para abordar este problema en las versiones 17.3, 16.7, 15.11, 14.16 y 13.19. Se recomienda en la mayor brevedad a los usuarios actualizar sus sistemas a estas versiones corregidas para mitigar el riesgo de explotación.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/postgresql-vulnerability-exploited.html

---

Vulnerabilidad crítica en Azure AI Face Service permite elevación de privilegios

Microsoft ha abordado recientemente una vulnerabilidad crítica en su servicio Azure AI Face Service, identificada como CVE-2025-21415. Esta falla, descubierta por un investigador anónimo, se debe a una omisión de autenticación mediante suplantación de identidad, lo que permite a un atacante autorizado elevar sus privilegios a través de la red. Con una puntuación CVSS de 9.9, esta vulnerabilidad representa un riesgo significativo para las organizaciones que utilizan este servicio.

Para mitigar este problema, Microsoft ha implementado actualizaciones de seguridad que abordan la vulnerabilidad. La compañía ha confirmado que ambas vulnerabilidades han sido completamente mitigadas y que los clientes no necesitan realizar ninguna acción adicional, ya que las actualizaciones de seguridad necesarias se han aplicado automáticamente. Se recomienda a los usuarios de Azure AI Face Service verificar que sus sistemas estén actualizados y seguir las directrices de seguridad proporcionadas por Microsoft para garantizar la protección continua de sus entornos

Prioridad: Crítico.

Ampliar Información:

https://sensorstechforum.com/es/cve-2025-21415-azure-ai-face-service/

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Malware FINALDRAFT explota la API de Microsoft Graph para espionaje en Windows y Linux

Investigadores de Elastic Security Labs han identificado una campaña de espionaje cibernético dirigida por el grupo REF7707, que ya afecta al Ministerio de Relaciones Exteriores de una nación sudamericana no especificada, así como a una entidad de telecomunicaciones y una universidad en el sudeste asiático. El malware, denominado FINALDRAFT, es un sofisticado troyano de administración remota escrito en C++ que permite a los atacantes ejecutar módulos adicionales y controlar sistemas comprometidos. Una característica notable de FINALDRAFT es su uso de la API de Microsoft Graph para el comando y control (C2), específicamente mediante el servicio de correo electrónico Outlook. El malware interactúa con la carpeta de borradores del buzón de correo para recibir comandos y almacenar los resultados de su ejecución, evitando así la detección al no enviar datos fuera de la red de manera convencional. Además, se ha detectado una

variante para Linux que mantiene funcionalidades similares de C2, lo que indica un esfuerzo coordinado y bien organizado por parte de los desarrolladores.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/finaldraft-malware-exploits-microsoft.html

---

Desarrolladores de Python afectados por malware disfrazado de paquete DeepSeek

Investigadores de Positive Technologies han identificado dos paquetes maliciosos en el repositorio de Python Package Index (PyPI), denominados 'deepseeek' y 'deepseekai', que se presentaban como recursos para integrar el modelo de inteligencia artificial chino DeepSeek en proyectos de software. Estos paquetes, subidos por un usuario llamado 'bvk' el 29 de enero de 2025, fueron detectados y eliminados por los administradores de PyPI en menos de una hora. Sin embargo, antes de su eliminación, fueron descargados más de 200 veces, principalmente en Sudamérica Y Norteamérica.

El malware oculto en estos paquetes estaba diseñado para recopilar datos del usuario y del sistema, incluyendo variables de entorno que a menudo contienen información sensible como claves API y credenciales de bases de datos. Los datos robados se enviaban a un servidor de comando y control a través de la plataforma de integración Pipedream. Se observó que el script malicioso fue escrito con la ayuda de un asistente de inteligencia artificial, evidenciado por comentarios característicos en el código. Para protegerse, se recomienda a los desarrolladores verificar la autenticidad de los paquetes antes de su instalación, revisar regularmente las dependencias de sus proyectos y emplear herramientas de seguridad para detectar posibles amenazas en el código.

Prioridad: Urgente.

Ampliar Información:

https://www.securityweek.com/developers-targeted-with-malware-disguised-as-deepseek-package/

Recomendaciones Generales Sobre Malware:

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Ataques whoAMI permiten a hackers ejecutar código en instancias de Amazon EC2

Investigadores de seguridad descubrieron una vulnerabilidad en Amazon Web Services (AWS) que permite a atacantes obtener acceso a cuentas mediante la publicación de una Amazon Machine Image (AMI) con un nombre específico. Denominado "whoAMI", este ataque explota la forma en que algunos proyectos de software recuperan los ID de las AMI, lo que puede llevar a la ejecución de código no autorizado en las instancias de Amazon EC2. Amazon confirmó la vulnerabilidad y lanzó una solución en septiembre de 2024; sin

embargo, el problema persiste en entornos donde los clientes no han actualizado su código.

Para mitigar este riesgo, se recomienda a las organizaciones revisar y actualizar sus procesos de selección de AMI, asegurándose de especificar el atributo 'owners' al buscar AMIs públicas para garantizar que provengan de fuentes confiables. Además, es crucial mantener el código y las configuraciones al día con las últimas actualizaciones de seguridad proporcionadas por AWS para prevenir posibles explotaciones de esta naturaleza.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/

Apple confirma explotación del Modo Restringido USB en ataque altamente sofisticado

Apple ha reconocido una vulnerabilidad crítica, identificada como CVE-2025-24200, que permite a atacantes con acceso físico a un iPhone o iPad bloqueado desactivar el Modo Restringido USB, una función clave de protección. Este fallo de seguridad fue descubierto por Bill Marczak del Citizen Lab de la Universidad de Toronto, y ha sido utilizado en "un ataque extremadamente sofisticado contra individuos específicos". La compañía ha abordado este problema en las actualizaciones iOS 18.3.1 y iPadOS 18.3.1.

El Modo Restringido USB, introducido en 2018, bloquea el acceso a datos a través del puerto Lightning o USB-C cuando el dispositivo ha estado bloqueado durante más de una hora, impidiendo que herramientas de hacking accedan al dispositivo sin autorización. La vulnerabilidad permitía a un atacante desactivar esta función sin necesidad de la contraseña, comprometiendo la seguridad del dispositivo. Se recomienda a todos los

usuarios actualizar sus dispositivos a las versiones más recientes de iOS y iPadOS para protegerse contra posibles explotaciones de esta naturaleza.

Prioridad: Importante.

Ampliar Información:

https://www.securityweek.com/apple-confirms-usb-restricted-mode-exploited-in-extremely-sophisticated-attack/