GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0424

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	4	2	1
MALWARE		4	1
NOTICIAS DE CIBERSEGURIDAD	1		3

VULNERABILIDADES

VMware confirma la explotación activa de una vulnerabilidad crítica en vCenter

VMware ha confirmado que una vulnerabilidad crítica de ejecución remota de código en vCenter Server, parcheada en octubre, está siendo activamente explotada. La plataforma vCenter Server es utilizada para gestionar entornos de VMware vSphere. La vulnerabilidad, identificada como CVE-2023-34048, permite la ejecución remota de código y fue reportada por el investigador de vulnerabilidades de Trend Micro Grigory Dorodnov. La explotación de esta vulnerabilidad no requiere autenticación ni interacción del usuario, lo que la hace especialmente peligrosa. VMware insta a los administradores a aplicar parches y, en caso de no ser posible, a controlar estrictamente el acceso a los componentes de gestión de vSphere en el perímetro de red.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/vmware-confirms-critical-vcenter-flaw-now-exploited-in-attacks/?&web_view=true

---

Fallas en PixieFail UEFI exponen a millones de computadoras a RCE, DoS y robo de datos

Se han revelado múltiples vulnerabilidades de seguridad en la pila de protocolos de red TCP/IP de una implementación de referencia de código abierto de la especificación Unified Extensible Firmware Interface (UEFI), utilizada ampliamente en computadoras modernas. Estas nueve vulnerabilidades, conocidas como PixieFail, residen en el TianoCore EFI Development Kit II (EDK II) y podrían ser explotadas para lograr ejecución remota de código, denegación de servicio (DoS), envenenamiento de caché DNS y filtración de información sensible. Las fallas afectan al firmware UEFI de AMI, Intel, Insyde y Phoenix Technologies, poniendo en riesgo a millones de dispositivos.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/pixiefail-uefi-flaws-expose-millions-of.html

---

Vulnerabilidades en dispositivos PAX POS basados en Android

Los dispositivos de punto de venta (POS) de PAX, basados en Android y ampliamente utilizados en bancos, presentan seis vulnerabilidades críticas. Descubiertas por el equipo de STM Cyber, estas vulnerabilidades permiten ejecución de código malicioso y escalada de privilegios, poniendo en peligro la seguridad de los sistemas utilizados en transacciones financieras. Las soluciones fueron comunicadas al fabricante en abril de 2023 y verificadas en noviembre de 2023.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.stmcyber.com/pax-pos-cves-2023/?web_view=true

Plataformas de IA y aprendizaje automático (ML) vulnerables: problemas críticos en MLflow, ClearML y Hugging Face

En el último mes, miembros de la plataforma de recompensas por errores Huntr identificaron vulnerabilidades severas en soluciones populares de inteligencia artificial y aprendizaje automático, como MLflow, ClearML y Hugging Face. MLflow presentó cuatro problemas críticos, incluyendo un fallo de travesía de ruta (CVE-2023-6831) y un bypass de validación de ruta (CVE-2023-6977), ambos con potencial para ejecución remota de código. Hugging Face Transformers tuvo un fallo crítico (CVE-2023-7018) que permitía a los atacantes lograr ejecución remota de código. Además, ClearML sufrió una falla de scripting entre sitios almacenada (XSS) de alta gravedad (CVE-2023-6778) en su componente de editor Markdown.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/critical-vulnerabilities-found-in-ai-ml-open-source-platforms/

Vulnerabilidades Zero-Day en Citrix NetScaler ADC y Gateway

Se ha descubierto la explotación en curso de dos vulnerabilidades zero-day en los productos Citrix NetScaler ADC y Gateway. Las vulnerabilidades, identificadas como CVE-2023-6548 y CVE-2023-6549, permiten la ejecución remota de código y ataques de denegación de servicio (DoS). CISA ha incluido estas vulnerabilidades en su catálogo de vulnerabilidades conocidas explotadas. Se insta a los usuarios a aplicar los parches disponibles de inmediato. La primera vulnerabilidad, CVE-2023-6548, es de gravedad media y permite la ejecución remota de código en la interfaz de gestión. La segunda, CVE-2023-6549, es de gravedad alta y puede ser explotada para ataques de DoS. Ambas afectan a los dispositivos gestionados por el cliente y no a los servicios en la nube de Citrix ni a las

Autenticaciones Adaptativas. CISA destaca la importancia de la separación del tráfico de la interfaz de gestión y aconseja no exponer dicha interfaz a internet.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/citrix-netscaler-zero-day-exploited/

Oracle corrige 200 vulnerabilidades en su actualización de enero de 2024

Oracle lanzó 389 parches en su primera Actualización Crítica de Parches de 2024 para abordar 200 vulnerabilidades. Con más de 200 problemas resueltos, se destaca Financial Services Applications con 71 parches. Oracle insta a los clientes a aplicar los parches rápidamente debido a la amenaza de explotación en la naturaleza. Se planean tres Actualizaciones Críticas más para 2024 en abril, julio y octubre.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/oracle-patches-200-vulnerabilities-with-january-2024-cpu/

Actualización Urgente para el Navegador Chrome ante la Explotación de una Vulnerabilidad Zero-Day

Google ha lanzado una actualización crítica para el navegador Chrome para abordar tres fallos de seguridad de alta gravedad. Una de las vulnerabilidades, CVE-2024-0519, es un zero-day que está siendo explotado activamente. El fallo se describe como un problema de acceso a la memoria fuera de límites en el motor JavaScript V8. Aunque Google no ha revelado detalles específicos sobre los ataques, se insta a los usuarios a actualizar sus navegadores rápidamente para mitigar el riesgo.

Esto sigue a los esfuerzos recientes de Google para parchear problemas de seguridad de memoria, con varios zero-days abordados en 2023.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/google-warns-of-chrome-browser-zero-day-being-exploited/

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

Alerta por Backdoor en Versiones Piratas de Software para macOS

Investigadores de Jamf Threat Labs encontraron aplicaciones pirateadas para macOS que incluyen un backdoor capaz de dar a los atacantes control remoto. Estas aplicaciones, alojadas en sitios chinos de piratería, contienen software legítimo como Navicat Premium y Microsoft Remote Desktop. Una vez ejecutado, el malware descarga y ejecuta cargas útiles para comprometer la máquina de la víctima. El backdoor, basado en la herramienta de postexplotación Khepri, se encuentra en "/tmp" y se borra al apagar el sistema.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/experts-warn-of-macos-backdoor-hidden.html?&web_view=true

---

Amenaza en npm: El paquete "oscompatible" instala AnyDesk eludiendo defensas

Un paquete malicioso en el registro npm, conocido como "oscompatible," ha sido identificado desplegando un troyano de acceso remoto en sistemas Windows comprometidos. Este paquete, retirado después de 380 descargas, ejecuta un script de compatibilidad antes de instalar AnyDesk y un troyano capaz de recopilar datos sensibles, resaltando los riesgos de seguridad en los ecosistemas de software de código abierto.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/npm-trojan-bypasses-uac-installs.html?&web_view=true

---

Hackers aprovechan el malware de la botnet Androxgh0st para robar credenciales de AWS y Microsoft

El FBI y CISA descubrieron una implementación activa del malware de la botnet Androxgh0st, diseñado para robar credenciales de AWS y Microsoft. El malware, escrito en Python, apunta a datos sensibles en archivos ".env," incluyendo credenciales para AWS, Office 365, SendGrid y Twilio. Androxgh0st utiliza diversas vulnerabilidades, como CVE-2017-9841 y CVE-2021-41773, para ejecutar código remoto, acceder a bases de datos y crear usuarios y políticas en sistemas comprometidos.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/androxgh0st-botnet-malware/

Remcos RAT se propaga a través de juegos para adultos en nueva ola de ataques

El troyano de acceso remoto (RAT) conocido como Remcos RAT se ha encontrado propagándose a través de servicios de almacenamiento en línea en Corea del Sur al hacerse pasar por juegos para adultos. Utilizando una técnica previamente empleada para distribuir otros tipos de malware, los atacantes engañan a los usuarios para que abran archivos maliciosos disfrazados de juegos para adultos en el servicio de almacenamiento web. Cuando se ejecutan, estos archivos lanzan scripts Visual Basic maliciosos que descargan e ejecutan el binario intermedio "ffmpeg.exe", que a su vez descarga Remcos RAT desde un servidor controlado por los atacantes. Remcos RAT, inicialmente comercializado como una herramienta legítima de administración remota, se ha convertido en una herramienta potente utilizada por actores maliciosos para el control remoto no autorizado de sistemas comprometidos.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2024/01/remcos-rat-spreading-through-adult.html

---

Malware Aprovecha 9Hits para Convertir Servidores Docker en Minadores de Criptomonedas y Generar Tráfico Web Falso

Investigadores de Cado Security han descubierto una nueva campaña que apunta a servidores Docker vulnerables, desplegando dos contenedores: un minador estándar XMRig y la aplicación 9Hits Viewer, un sistema automatizado de intercambio de tráfico. Los ciberdelincuentes utilizan la aplicación 9Hits Traffic Exchange Viewer como carga útil, lo que marca el primer caso documentado de malware que utiliza esta aplicación con ese propósito. La campaña impacta significativamente los servidores comprometidos, agotando los recursos de la CPU y afectando las cargas de trabajo legítimas. Los atacantes explotan servidores Docker vulnerables, utilizando imágenes populares de Dockerhub para sus ataques.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hackread.com/docker-servers-malware-traffic-boosted-cryptominers/?web_view=true#google_vignette

---

Recomendaciones generales sobre Malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.

- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

Hackeo de cuentas de Payoneer en Argentina con bypass de 2FA

Numerosos usuarios de Payoneer en Argentina informan que, tras recibir códigos OTP por SMS mientras dormían, sus cuentas protegidas con autenticación de dos factores (2FA) fueron hackeadas y sus fondos robados. Payoneer, una plataforma de servicios financieros, es popular en Argentina por permitir a las personas ganar en monedas extranjeras eludiendo las regulaciones bancarias locales. Los afectados recibieron solicitudes de aprobación para restablecer la contraseña antes del ataque. Se sospecha de un posible fallo en la seguridad de Payoneer o una violación de datos en el proveedor de SMS. Payoneer atribuye el incidente a la supuesta interacción de los usuarios con enlaces de phishing, mientras que estos niegan haber hecho clic, generando controversia sobre la responsabilidad.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/payoneer-accounts-in-argentina-hacked-in-2fa-bypass-attacks/?&web_view=true

---

Hackers rusos roban correos corporativos de Microsoft en una brecha que duró un mes

Microsoft informó el viernes pasado que algunos de sus correos corporativos fueron violados y datos robados por un grupo de hackers respaldado por el estado ruso conocido como Midnight Blizzard. La brecha, descubierta el 12 de enero, reveló que los atacantes, también llamados Nobelium o APT29,

accedieron mediante un ataque de fuerza bruta a una cuenta de prueba no productiva. Aunque Microsoft no reveló el impacto total, confirmó que se robaron correos electrónicos y archivos de cuentas corporativas, incluidas las de su equipo directivo y empleados de ciberseguridad y legal. La compañía señaló que la brecha no fue causada por una vulnerabilidad en sus productos, sino por una contraseña débil sin autenticación de dos factores.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/russian-hackers-stole-microsoft-corporate-emails-in-month-long-breach/?&web_view=true

---

Ataques de Ransomware utilizan TeamViewer para acceder a redes

Actores de ransomware están utilizando nuevamente TeamViewer para obtener acceso inicial a los puntos finales de las organizaciones e intentar implementar cifradores basados en el constructor de ransomware LockBit filtrado. TeamViewer, una herramienta legítima de acceso remoto, es apreciada en el mundo empresarial por su simplicidad y capacidades. Huntress ha informado que los atacantes están utilizando técnicas antiguas para tomar el control de dispositivos a través de TeamViewer y desplegar ransomware. Los intentos de despliegue de ransomware se basan en el constructor filtrado de LockBit 3.0. Huntress no ha podido atribuir con certeza los ataques a grupos conocidos de ransomware, pero señala similitudes con el modus operandi de LockBit. Se destaca la importancia de mantener fuertes prácticas de seguridad, como contraseñas complejas, autenticación de dos factores y actualizaciones regulares del software.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/teamviewer-abused-to-breach-networks-in-new-ransomware-attacks/?&web_view=true#google_vignette

---

Los scripts iShutdown pueden ayudar a detectar spyware en iOS en tu iPhone

Los investigadores de seguridad descubrieron que infecciones con spyware de alto perfil como Pegasus, Reign y Predator podrían ser descubiertas en dispositivos móviles de Apple comprometidos al verificar Shutdown.log, un archivo de registro del sistema que almacena eventos de reinicio. Kaspersky ha lanzado scripts en Python para ayudar a automatizar el proceso de análisis del archivo Shutdown.log y reconocer posibles signos de infección por malware de una manera fácil de evaluar. Estos scripts analizan el archivo Sysdiagnose y extraen artefactos del registro de reinicio para facilitar la detección de malware en dispositivos iOS. La técnica proporciona un método de análisis mucho más fácil en comparación con técnicas estándar como examinar una copia de seguridad encriptada de iOS o el tráfico de red. Los investigadores recomiendan reiniciar el dispositivo con frecuencia para obtener datos relevantes del archivo de registro de reinicio.

Prioridad: 3 Importante.

Ampliar información:

- h https://www.bleepingcomputer.com/news/security/ishutdown-scripts-can-help-detect-ios-spyware-on-your-iphone/#google_vignette