GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4324

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

VULNERABILIDADES

Vulnerabilidad en CPUs Intel y AMD en Linux por Evasión de Spectre

Investigadores de ETH Zurich han descubierto una vulnerabilidad crítica que afecta tanto a procesadores Intel como AMD en sistemas Linux. Este problema, catalogado bajo los CVE-2023-38575 (Intel) y CVE-2022-23824 (AMD), permite a los atacantes eludir las mitigaciones implementadas para Spectre. La vulnerabilidad se aprovecha de la predicción de operaciones de los procesadores, lo que puede resultar en la exposición de información sensible almacenada en la memoria.

Esta nueva falla destaca por su capacidad de comprometer datos a pesar de las protecciones previas aplicadas para mitigar sus ataques, lo que plantea un desafío significativo para la seguridad informática en sistemas basados en Linux que utilicen estos chips, se recomienda monitorear el impacto de esta vulnerabilidad en entornos de alto riesgo, como servidores y sistemas críticos, donde la exposición a datos sensibles puede ser devastadora.

Prioridad: 1 crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/intel-amd-cpus-on-linux-impacted-by-newly-disclosed-spectre-bypass/

Vulnerabilidad crítica en Kubernetes expone nodos a acceso raíz

Una nueva vulnerabilidad, CVE-2024-9486, afecta al Kubernetes Image Builder, principalmente con el proveedor Proxmox. Esta falla deja credenciales predeterminadas activas tras crear imágenes de máquinas virtuales, lo que abre la puerta a un atacante para acceder a los nodos con privilegios de root. Es un riesgo crítico que afecta a nodos mal configurados.

Se recomienda deshabilitar las cuentas predeterminadas y actualizar a la versión 0.1.38 del Image Builder para mejorar la seguridad. La actualización permite reconstruir las imágenes del sistema, cerrando posibles vulnerabilidades que puedan ser explotadas por atacantes. Este proceso es esencial para prevenir accesos no autorizados, asegurando que los entornos afectados estén protegidos frente a amenazas de seguridad.

Prioridad: 2 urgente.

Ampliar información:

https://thehackernews.com/2024/10/critical-kubernetes-image-builder.html

---

Vulnerabilidad en macOS utilizada por adware Adload

Microsoft descubrió una vulnerabilidad en macOS, CVE-2024-44133, que permite al adware Adload eludir el sistema de Transparencia, Consentimiento y Control (TCC). Los atacantes pueden acceder a funciones como la cámara y el micrófono sin autorización, comprometiendo la seguridad de los usuarios de macOS.

Apple lanzó una actualización para corregir esta vulnerabilidad en macOS Sequoia 15. Se recomienda que los usuarios actualicen sus sistemas a la última versión y monitoreen cualquier comportamiento anómalo de sus aplicaciones para prevenir posibles ataques de adware.

Prioridad: 2 urgente.

Ampliar información:

https://www.securityweek.com/microsoft-macos-vulnerability-potentially-exploited-in-adware-attacks/

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 fortalecer la seguridad de los sistemas.

MALWARE

Malware disfrazado de errores de Google Meet roba información confidencial

Un grupo de ciberdelincuentes, identificado como TA571, está utilizando correos electrónicos fraudulentos que aparentan ser errores de conexión de Google Meet para distribuir malware de robo de información. Los correos incitan a las víctimas a ejecutar comandos maliciosos en PowerShell, lo que resulta en la descarga de malware como Stealc y Rhadamanthys, que pueden robar credenciales, datos del navegador y archivos sensibles.

Este ataque fue identificado por Proofpoint. Se recomienda no ejecutar comandos no verificados, evitar enlaces sospechosos y mantener actualizado el software de seguridad para prevenir infecciones por malware.

Prioridad: 2 urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/fake-google-meet-conference-errors-push-infostealing-malware/

RomCom ataca entidades ucranianas y polacas con nuevo malware SingleCamper

El grupo de origen ruso RomCom ha lanzado ataques de espionaje contra gobiernos y organizaciones en Ucrania y Polonia utilizando una nueva variante de su malware, SingleCamper RAT. Los ataques se propagan a través de correos electrónicos de spear-phishing que contienen documentos señuelo diseñados para descargar el malware, que realiza reconocimiento de red y robo de datos.

Identificado por Cisco Talos, este malware se utiliza para espionaje, con capacidades avanzadas de persistencia y exfiltración de datos. Se recomienda implementar monitoreo de red y segmentación para mitigar el riesgo.

Prioridad: 3 importante.

Ampliar información:

https://thehackernews.com/2024/10/russian-romcom-attacks-target-ukrainian.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.

Recomendación adicional: Educar a los empleados o usuarios sobre ciberseguridad, para que puedan reconocer y evitar posibles amenazas como el malware o ataques de ingeniería social.

Microsoft pierde registros de seguridad de clientes durante un mes

Microsoft informó que un error en la recopilación de registros de seguridad en varios servicios de Azure resultó en la pérdida de datos críticos durante septiembre y octubre de 2024. Esto afectó la capacidad de los clientes para detectar posibles amenazas, comprometiendo servicios como Microsoft Entra y Microsoft Sentinel.

Microsoft ha solucionado el problema, pero recomienda a los clientes revisar sus configuraciones de seguridad, monitorear los servicios afectados y realizar auditorías de los registros de seguridad para evitar posibles brechas en el futuro.

Prioridad: 3 importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/microsoft-warns-it-lost-some-customers-security-logs-for-a-month/

Cisco desactiva DevHub tras la filtración de datos

Cisco desconectó su portal DevHub después de que el grupo de hackers IntelBroker publicara datos robados del entorno de desarrollo de terceros. El grupo accedió al portal mediante un token API expuesto, obteniendo código fuente y archivos de configuración, lo cual fue divulgado en foros de hackers.

Cisco está investigando el incidente y ha bloqueado el acceso al portal afectado. Se recomienda a las empresas revisar sus entornos de desarrollo y aplicar políticas estrictas de seguridad en el manejo de tokens API para evitar futuras brechas.

Prioridad: 3 importante.

Ampliar información:

https://www. https://www.bleepingcomputer.com/news/security/cisco-takes-devhub-portal-offline-after-hacker-publishes-stolen-data/