GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °3123

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	5	2	
MALWARE	1	1	1
BRECHAS DE SEGURIDAD			1
NOTICIAS DE CIBERSEGURIDAD		1	4

VULNERABILIDADES

Google revela ataques 'Downfall' y vulnerabilidad en chips Intel

Google ha revelado una vulnerabilidad en procesadores Intel, llamada "Downfall", que permite ataques de robo de datos. La vulnerabilidad, CVE-2022-40982, afecta a procesadores Core de sexta a undécima generación. Daniel Moghimi de Google descubrió que los atacantes pueden explotar una instrucción llamada "gather" para robar datos de otros usuarios en el mismo CPU. Intel ha lanzado parches de microcódigo para mitigar el problema, pero podrían reducir el rendimiento en algunas cargas de trabajo.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.techtarget.com/searchsecurity/news/366547448/Google-unveils-Downfall-attacks-vulnerability-in-Intel-chips
- https://briefly.co/anchor/Information_security/story/downfall-vulnerability-affects-millions-of-intel-cpus-with-strong-data-leak-impact?hl=1&f=porchetta&utm_source=Twitter&utm_medium=autotweet&utm_content=unhighlighted&utm_campaign=Information_security

---

Divulgación de información de Adobe Acrobat y Adobe Reader (CVE-2023-38237)

Se ha detectado una vulnerabilidad en Adobe Acrobat y Adobe Reader que podría permitir a un atacante remoto acceder a información confidencial mediante una lectura fuera de los límites habituales. Esta vulnerabilidad requiere la interacción del usuario al abrir un documento manipulado. Es importante aplicar las actualizaciones pertinentes para evitar posibles explotaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/adobe-acrobat-and-adobe-reader-information-disclosure-cve-2023-38237/

Múltiples fallas encontradas en el tema y complemento de WordPress de Avada

Se han descubierto múltiples vulnerabilidades en el ampliamente utilizado tema Avada y su complemento Avada Builder en WordPress. Estos fallos de seguridad, revelados por el investigador de seguridad de Patchstack Rafie Muhammad, exponen a un número significativo de sitios web de WordPress a posibles brechas. El complemento Avada Builder presenta dos debilidades: una inyección SQL autenticada y una vulnerabilidad de Cross-Site Scripting (XSS) reflejada. Patchstack también identificó varias vulnerabilidades en el tema Avada, incluyendo la capacidad de cargar archivos arbitrarios y la posibilidad de ejecución remota de código. Estas vulnerabilidades fueron

reportadas al proveedor y se recomienda a los usuarios actualizar a las versiones corregidas para mantener la seguridad del sitio web.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.infosecurity-magazine.com/news/flaws-wordpress-avada-theme-plugin/?&web_view=true

---

El ataque al carrito de compra de Magento apunta a una vulnerabilidad crítica revelada a principios de 2022

Las tiendas de comercio electrónico que usan Magento 2 de Adobe enfrentan un ataque por una vulnerabilidad crítica parcheada en 2022. Investigadores de Akamai descubrieron una campaña de inyección de plantillas en el lado del servidor, dirigida a tiendas Magento 2 que aún no han abordado la falla CVE-2022-24086. Los atacantes intentan robar estadísticas de pago de pedidos recientes. A pesar de ser parcheada, esta campaña subraya cómo las vulnerabilidades antiguas siguen siendo explotadas debido a la dificultad de mantener parches y medidas de seguridad actualizadas en las empresas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.theregister.com/2023/08/11/magento_shopping_cart_attack_targets/?&web_view=true

---

Nuevas vulnerabilidades de día cero podrían drenar instantáneamente las billeteras criptográficas

En la conferencia Black Hat USA se revelaron múltiples vulnerabilidades de día cero en protocolos criptográficos de computación multiparte (MPC) ampliamente utilizados. Estas vulnerabilidades, conocidas como BitForge, podrían permitir a los atacantes vaciar carteras de criptomonedas en segundos si no se corrigen. Aunque no se ha detectado explotación, la preocupación radica en la dificultad de detección si se roba una clave privada. Los proveedores de carteras como Coinbase WaaS, Zengo y Binance podrían ser impactados. Fireblocks trabajó en soluciones y destaca la importancia de la seguridad en el software de criptomonedas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.infosecurity-magazine.com/news/zero-day-vulnerabilities-crypto/?&web_view=true

---

Múltiples vulnerabilidades en PostgreSQL

Estas vulnerabilidades afectan a las versiones anteriores a 15.4, 14.9, 13.12, 12.16 y 11.21, permitiendo a un atacante ejecutar código arbitrario y eludir políticas de seguridad. Se recomienda a los usuarios afectados aplicar los parches proporcionados por PostgreSQL. Las referencias CVE asociadas a estas vulnerabilidades son CVE-2023-39417 y CVE-2023-39418.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0651/

Múltiples vulnerabilidades en Microsoft Office

Estas vulnerabilidades afectan a diversas versiones de Microsoft 365 Apps, Excel, Office, Outlook y otras, permitiendo a un atacante ejecutar código arbitrario a distancia y realizar usurpación de

identidad. Se recomienda a los usuarios afectados aplicar los parches proporcionados por Microsoft. Las referencias CVE asociadas a estas vulnerabilidades incluyen CVE-2023-36895, CVE-2023-35371, CVE-2023-35372, CVE-2023-36866, CVE-2023-36865, CVE-2023-36893 y CVE-2023-36896.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0641/

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

Clop ransomware ahora usa torrents para filtrar datos y evadir takedowns

El grupo de ransomware Clop ha modificado sus tácticas de extorsión y ahora está utilizando torrents para filtrar datos robados en ataques MOVEit. Empezando el 27 de mayo, el grupo Clop explotó una vulnerabilidad zero-day en la plataforma de transferencia de archivos seguros MOVEit para robar datos de casi 600 organizaciones en todo el mundo. Luego, el 14 de junio, comenzaron a extorsionar a las víctimas, publicando lentamente los nombres en su sitio de filtración de datos en Tor y finalmente liberando públicamente los archivos. Para mejorar la velocidad de descarga, Clop ha recurrido a torrents para distribuir los datos robados de los ataques MOVEit.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/

La nueva variante de Yashma Ransomware se dirige a varios países de habla inglesa

Se ha descubierto que un actor de amenazas desconocido utiliza una variante del ransomware Yashma para atacar entidades en países de habla inglesa, Bulgaria, China y Vietnam desde junio de 2023. Cisco Talos atribuye la operación a un adversario de origen vietnamita. El ransomware utiliza una técnica inusual para entregar la nota de rescate, descargándola de un repositorio GitHub controlado por el actor. El ransomware Yashma es una versión renombrada de otro llamado Chaos. La nota de rescate se asemeja al ransomware WannaCry. Este aumento en variantes de ransomware se relaciona con filtraciones de código fuente, y los ataques de ransomware han aumentado significativamente.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/new-yashma-ransomware-variant-targets-multiple-english-speaking-countries/

Los operadores de malware QakBot amplían la red C2 con 15 nuevos servidores

Los operadores detrás del malware QakBot han expandido su red de servidores de comando y control (C2) con 15 nuevos servidores a finales de junio de 2023. Esto se produce después de un análisis de la infraestructura del malware realizado por Team Cymru. La red C2 de QakBot se comunica en niveles, y estos nuevos servidores se conectan con nodos C2 de nivel 2 (T2) en proveedores de VPS geolocalizados en Rusia. Aunque los operadores de QakBot suelen tomar un descanso durante el verano, este período podría estar siendo utilizado para mejorar y actualizar su infraestructura.

Prioridad: 3 Importante.

Ampliar información:

- https://www.redpacketsecurity.com/qakbot-malware-operators-expand-c-network-with-new-servers/

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.

BRECHAS DE SEGURIDAD

Una brecha en la Comisión Electoral del Reino Unido expone los datos de 40 millones de votantes británicos

La Comisión Electoral del Reino Unido ha sufrido un ciberataque que expuso los datos de 40 millones de votantes. El ataque pasó desapercibido por más de un año y permitió a los ciberdelincuentes acceder a servidores de correo electrónico y registros electorales. Los datos comprometidos incluyen nombres, direcciones de correo electrónico, números de teléfono y más. Aunque no se conoce la identidad de los atacantes, la Comisión está tomando medidas para mitigar futuros ataques y asegura que el incidente no afecta al proceso electoral ni al censo electoral.

Prioridad: 3 Importante.

Ampliar información:

- https://derechodelared.com/comision-electoral-datos-40-millones-votantes/

NOTICIAS DE CIBERSEGURIDAD

Han descubierto un truco con el que puedes instalar Windows 11 sin el montón de aplicaciones preinstaladas que nos cuela Microsoft

Se ha descubierto un truco que permite a los usuarios instalar Windows 11 sin las aplicaciones preinstaladas que Microsoft incluye en el sistema operativo. Estas aplicaciones a menudo se conocen como "bloatware" y pueden incluir software de terceros como TikTok, Candy Crush e

Instagram. El truco implica seleccionar la opción "English (World)" o "English (European)" durante el proceso de instalación, lo que desencadena un error llamado "OOBEREGION". A pesar del error, al seleccionar "Skip", se logra una instalación limpia de Windows 11 con solo las aplicaciones esenciales. Sin embargo, Microsoft podría corregir este truco en futuras actualizaciones del sistema operativo.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/windows/han-descubierto-truco-que-puedes-instalar-windows-11-monton-aplicaciones-preinstaladas-que-nos-cuela-microsoft

---

Cómo conocer todos los datos personales que Google tiene en su registro

Se destaca cómo Google recopila datos personales a través de varios productos y cómo los usuarios pueden ver y gestionar esta información mediante el Panel de Control y la configuración de la cuenta. También se menciona la opción de planificar el destino de la cuenta en caso de fallecimiento o eliminarla por completo. Aunque estas herramientas aún no están disponibles en todos los lugares, se plantea la pregunta de si los usuarios se atreverán a ver cuánta información tiene Google sobre ellos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/paso-a-paso/unos-pocos-clics-puedes-ver-todos-datos-personales-que-google-tiene-ti-que-quizas-sepas-1

Project IDX es el nuevo rival para Visual Studio Code, creado por Google y con inteligencia artificial integrada

Google ha lanzado Project IDX, un entorno de desarrollo integrado basado en la nube que incorpora inteligencia artificial y tiene como objetivo competir con Visual Studio Code de Microsoft. Project IDX se ejecuta en un navegador web y se beneficia de Google Cloud, y se distingue por su integración con Codey, un modelo de inteligencia artificial diseñado para tareas de programación. Esta herramienta proporciona características como importación fácil de proyectos, compatibilidad con diversos frameworks y lenguajes, sugerencias de código inteligentes, visualización en la nube y despliegue simplificado con Firebase.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/desarrollo/project-idx-nuevo-rival-para-visual-studio-code-creado-google-inteligencia-artificial-integrada

---

Interpol desmantela la plataforma de phishing como servicio "16shop"

INTERPOL ha desmantelado la plataforma de phishing "16shop" en una operación internacional. Esta plataforma ofrecía "kits de phishing" a ciberdelincuentes para realizar estafas por correo electrónico. El operador principal y un colaborador fueron arrestados. La colaboración con fuerzas de seguridad y empresas de ciberseguridad fue clave. El phishing sigue siendo una amenaza grave y la colaboración internacional es vital para combatirla.

Prioridad: 3 Importante.

Ampliar información:

- https://derechodelared.com/phishing-as-a-service-16shop-interpol/

El nuevo ataque acústico roba datos de las pulsaciones de teclas con una precisión del 93%

Investigadores británicos han creado un modelo de aprendizaje profundo que puede robar datos de pulsaciones de teclado con un micrófono, con una precisión del 95%. Incluso utilizando Zoom, lograron una precisión del 93%. Este ataque acústico compromete la seguridad al filtrar contraseñas y datos confidenciales. A diferencia de otros ataques, no requiere condiciones especiales y es más factible debido a la abundancia de micrófonos en dispositivos. Recomiendan la autenticación biométrica y el uso de administradores de contraseñas para mitigar este riesgo.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/new-acoustic-attack-steals-data-from-keystrokes-with-accuracy/