GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4823

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	3	2	
MALWARE	1	3	2
NOTICIAS DE CIBERSEGURIDAD		2	2

VULNERABILIDADES

Dos nuevas vulnerabilidades reveladas en MOVEit de Progress Software

Progress Software ha anunciado dos nuevas vulnerabilidades de alta gravedad en su servicio de transferencia de archivos MOVEit. Las vulnerabilidades, identificadas como escalada de privilegios (CVE-2023-6218) y scripting entre sitios (CVE-2023-6217), fueron parcheadas el 29 de noviembre. Estos hallazgos elevan el total de CVEs en MOVEit a ocho desde que una vulnerabilidad de día cero, CVE-2023-34362, fue explotada masivamente a finales de mayo. Aunque no hay evidencia de explotación activa de las nuevas vulnerabilidades, Progress Software ha experimentado ataques relacionados con el ransomware Clop, afectando a casi 2.700 organizaciones y más de 84 millones de personas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cybersecuritydive.com/news/progress-software-moveit-cves/701889/?&web_view=true

---

Vulnerabilidades en routers Sierra Wireless exponen sectores críticos a ataques cibernéticos

Un total de 21 vulnerabilidades, denominadas Sierra:21, han sido descubiertas en routers celulares Sierra Wireless AirLink y en software de código abierto como TinyXML y OpenNDS. Forescout Vedere Labs advierte que estas fallas comprometen más de 86.000 dispositivos en sectores críticos, como energía y salud. Entre las vulnerabilidades, una es crítica, nueve son de alta gravedad y 11 son de gravedad media, permitiendo a los atacantes robar credenciales, tomar control del router e infiltrarse en redes críticas. Las correcciones han sido lanzadas, pero la necesidad de abordar problemas en TinyXML recae en los vendedores afectados. Forescout destaca el riesgo de ataques de malware de botnet, instando a la vigilancia y protección ante posibles consecuencias como interrupciones y espionaje.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/12/sierra21-flaws-in-sierra-wireless.html

---

Vulnerabilidades en módems 5G afectan a dispositivos iOS y Android

Una serie de fallos de seguridad en la implementación del firmware de los módems de red móvil 5G de importantes proveedores de chipsets como MediaTek y Qualcomm afectan a modems USB, IoT y cientos de modelos de smartphones que ejecutan Android e iOS. Estas 14 vulnerabilidades, colectivamente denominadas 5Ghoul, impactan a 714 smartphones de 24 marcas, incluyendo Vivo, Xiaomi, OPPO, Samsung, Apple, entre otras. Diez de los fallos afectan a los módems 5G de MediaTek y Qualcomm, destacando tres como de alta severidad. Estos fallos podrían ser explotados para lanzar ataques que desconecten o congelen la conexión, incluso degradar la conectividad 5G a 4G.

Aunque se han lanzado parches para 12 de las vulnerabilidades, la demora en la implementación de actualizaciones de seguridad 5G podría exponer a los usuarios a riesgos durante meses.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/12/new-5g-modems-flaws-affect-ios-devices.html

---

Vulnerabilidad en cadena POP de WordPress expone a más de 800 millones de sitios a ataques

La versión 6.4.2 de WordPress aborda una vulnerabilidad crítica de ejecución remota de código en la cadena POP, introducida en la versión 6.4. Esta falla, combinada con una Inyección de Objetos, permitiría la ejecución de código PHP arbitrario. Aunque no se ha asignado un CVE, WordPress insta a la actualización para evitar posibles ataques de toma de control. La vulnerabilidad reside en la clase WP_HTML_Token, utilizada en el editor de bloques. Se recomienda a los usuarios actualizar a la versión 6.4.2 para prevenir la explotación de esta amenaza.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/wordpress-pop-chain-flaw/

Aumento en la explotación de vulnerabilidades recientes en Cisco IOS XE

La Fundación Shadowserver advierte sobre un aumento en la cantidad de dispositivos comprometidos a través de vulnerabilidades recientemente corregidas en Cisco IOS XE. Las fallas, identificadas como CVE-2023-20198 y CVE-2023-20273, fueron parcheadas en octubre, pero los atacantes las están utilizando para crear cuentas privilegiadas y desplegar implantes maliciosos. La Fundación ha detectado más de 23.000 dispositivos afectados, sugiriendo una posible nueva

campaña de ataque. Se insta a las organizaciones a aplicar los parches correspondientes y buscar actividad maliciosa en sus redes.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/exploitation-of-recent-cisco-ios-xe-vulnerabilities-spikes/

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

Malware SpyLoan para Android se dirige a usuarios del sudeste asiático, África y América Latina

ESET ha identificado SpyLoan, un malware que se disfraza como aplicaciones de préstamos en Android, comprometiendo la privacidad al recopilar datos sensibles. Este riesgo afecta a usuarios en el sudeste asiático, África y América Latina, subrayando la importancia de la precaución al descargar aplicaciones financieras en estas regiones. SpyLoan, camuflado como servicios legítimos, no solo ofrece préstamos con tasas de interés exorbitantes, sino que también roba información personal para chantajear a los usuarios. La detección temprana y la conciencia son fundamentales para protegerse contra esta amenaza emergente en el panorama de ciberseguridad móvil.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.welivesecurity.com/en/eset-research/beware-predatory-fintech-loan-sharks-use-android-apps-reach-new-depths/?&web_view=true

---

Headcrab infecta servidores Redis con nueva variante

El malware 'HeadCrab' regresa con fuerza al infectar 1.100 servidores con su segunda variante, sumándose a los 1.200 afectados por la primera. Aunque no es un rootkit convencional, su capacidad de controlar funciones y respuestas lo hace invisible. La nueva versión mejora la capacidad de ocultar acciones al eliminar comandos personalizados y agregar cifrado.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.darkreading.com/cyberattacks-data-breaches/headcrab-malware-variants-commandeer-thousands-of-servers?&web_view=true

---

COLDRIVER: Microsoft advierte sobre nuevas tácticas de evasión y robo de credenciales

Microsoft alerta que COLDRIVER, conocido como Star Blizzard, continúa perfeccionando sus tácticas de robo de credenciales y evasión de detección. El grupo, vinculado al FSB ruso, se destaca por suplantar páginas de inicio de sesión. A pesar de sanciones recientes, COLDRIVER persiste en dirigirse a entidades estratégicas para Rusia. Microsoft observa nuevas técnicas, como el uso de scripts del lado del servidor y servicios de marketing por correo electrónico, para redirigir a las víctimas a páginas de phishing. El grupo sigue enfocado en el robo de credenciales de correo electrónico, especialmente dirigido a proveedores basados en la nube.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/12/microsoft-warns-of-coldrivers-evolving.html

---

GuLoader refina técnicas anti-análisis para desafiar la seguridad

El malware GuLoader ha actualizado sus tácticas anti-análisis, dificultando la detección y el estudio. Aunque su funcionalidad central no ha cambiado, las mejoras en las técnicas de ofuscación hacen que analizar GuLoader sea un proceso más complejo y demorado. Este malware basado en shellcode se utiliza para distribuir diversas cargas maliciosas, incluyendo robar información, empleando estrategias avanzadas para evadir las soluciones de seguridad tradicionales. Su propagación común ocurre a través de campañas de phishing, utilizando archivos ZIP o enlaces con scripts de Visual Basic. Las actualizaciones recientes incluyen refinamientos en la técnica anti-análisis basada en Vectored Exception Handling (VEH), acentuando la adaptabilidad de GuLoader para eludir la detección y resistir el análisis de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/12/researchers-unveal-guloader-malwares.html

---

Nuevo malware dirigido a usuarios de MacOS

Se ha descubierto un nuevo troyano dirigido a usuarios de macOS, asociado al grupo APT BlueNoroff y su campaña RustBucket. Este grupo, vinculado a Lazarus, destaca por su experiencia en ingeniería inversa y su enfoque en ataques financieros, incluyendo el robo al Banco Central de Bangladesh. La nueva variante del cargador se distribuyó a través de un archivo PDF falso y utiliza un ejecutable escrito en Swift. Aunque aún se desconoce la forma exacta de distribución, el malware espera comandos del servidor, y la mayoría de los antivirus actualmente pueden detectarlo.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/bluenoroff-macos-users/#google_vignette

---

Se descubren nuevas técnicas de inyección de procesos en Windows

SafeBreach ha revelado ocho nuevas técnicas de inyección de procesos llamadas "Pool Party". Estas variantes aprovechan los Windows thread pools para ejecutar código malicioso como resultado de acciones legítimas, siendo completamente indetectables por las principales soluciones de detección y respuesta de endpoint (EDR).

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/new-pool-party-process-injection-techniques-undetected-by-edr-solutions/

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

Hackeando la mente humana: explotando vulnerabilidades en la primera línea de defensa cibernética

En el dinámico mundo de la ciberseguridad, los humanos siguen siendo objetivos primarios para los atacantes. Este artículo explora cómo los ciberdelincuentes han perfeccionado el arte de explotar las complejidades de la mente humana, manipulando sesgos y desencadenantes emocionales para comprometer la seguridad personal y organizacional. Al destacar la complejidad de la mente humana, se resalta cómo los atacantes aprovechan rasgos fundamentales como la confianza, la empatía y la urgencia. Se aborda la necesidad de alinearse cognitivamente con los desencadenantes emocionales para prevenir reacciones impulsivas y se promueve una mentalidad de "detener y evaluar" como una barrera mental contra ataques de ingeniería social. La conciencia y la colaboración proactiva se presentan como herramientas clave para mitigar amenazas.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/12/hacking-human-mind-exploiting.html?&web_view=true

---

Google abandona contraseñas y adopta passkeys para mayor seguridad

Google ha anunciado un cambio significativo en la seguridad de inicio de sesión, reemplazando las contraseñas con passkeys de forma predeterminada. La passkey, una credencial digital vinculada a métodos de desbloqueo de dispositivos, como códigos PIN o datos biométricos, busca hacer que las contraseñas sean obsoletas. Proporciona una capa adicional de seguridad, ya que un atacante necesitaría acceso físico al dispositivo del usuario. Google afirma que este método es un 40% más rápido y resistente a la suplantación de identidad. Aunque las contraseñas seguirán siendo una opción, el movimiento de Google podría acelerar la transición hacia un internet más seguro, con otras grandes empresas siguiendo su ejemplo.

Prioridad: 3 Importante.

Ampliar información:

- https://www.pandasecurity.com/es/mediacenter/passkey-google-anuncia-fin-contrasena/

Nuevo ataque utiliza IA para evadir protecciones en modelos de lenguaje grandes como gpt-4

Investigadores de Robust Intelligence y la Universidad de Yale han revelado un nuevo método automatizado de aprendizaje automático adversarial que logra evadir las protecciones de modelos avanzados, como GPT-4, de manera exitosa y sin supervisión humana. Llamado "Tree of Attacks with Pruning" (TAP), este método puede utilizarse para inducir a modelos sofisticados a generar cientos de respuestas tóxicas o dañinas a consultas de usuarios en minutos, superando las salvaguardas implementadas por desarrolladores. La vulnerabilidad parece ser universal en tecnología de

modelos de lenguaje y presenta desafíos significativos para abordarla de manera fundamental. Los hallazgos instan a los desarrolladores a comprender y mitigar este riesgo en tiempo real.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.robustintelligence.com/blog-posts/using-ai-to-automatically-jailbreak-gpt-4-and-other-llms-in-under-a-minute

---

La Unión Europea alcanza un acuerdo histórico sobre las primeras reglas de inteligencia artificial a nivel mundial

La Unión Europea (UE) ha alcanzado un acuerdo sobre las primeras normas de inteligencia artificial (IA) a nivel mundial, conocido como el "Artificial Intelligence Act". Este acuerdo allana el camino para la supervisión legal de la tecnología de IA, que ha prometido transformar la vida cotidiana y ha generado advertencias sobre peligros existenciales para la humanidad. Los negociadores superaron diferencias en puntos controvertidos, como la IA generativa y el uso policial de la vigilancia de reconocimiento facial. Aunque grupos de la sociedad civil critican que el acuerdo no protege lo suficiente a las personas de los daños causados por sistemas de IA, el Parlamento Europeo deberá votar sobre el acto a principios del próximo año para que entre en vigencia.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/europe-reaches-a-deal-on-the-worlds-first-comprehensive-ai-rules/
