GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4524

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	3	0	0
MALWARE	0	1	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Yahoo revela vulnerabilidades críticas en NetIQ iManager que permiten ejecución remota de código

El equipo de investigación de Yahoo!, ha descubierto 11 vulnerabilidades significativas en NetIQ iManager, una herramienta de gestión de directorios utilizada por empresas. Entre las más peligrosas se encuentran: CVE-2024-3487 (omisión de autenticación), CVE-2024-3483 (inyección de comandos), CVE-2024-3488 (carga arbitraria de archivos) y CVE-2024-4429 (omisión de validación CSRF). Estas fallas pueden ser explotadas de forma combinada para lograr la ejecución remota de código sin necesidad de autenticación, lo que permitiría a un atacante tomar el control de la herramienta y robar credenciales de administrador.

Para mitigar estos riesgos, OpenText ha emitido actualizaciones críticas en abril de 2024. Se invita a los usuarios a instalar estas correcciones de inmediato y a reforzar las configuraciones de seguridad del software para proteger las redes corporativas de posibles ataques. Además, se recomienda revisar las prácticas de seguridad generales y asegurar que los accesos administrativos estén protegidos con mecanismos de autenticación robusta.

Prioridad: Crítico.

Ampliar información:

https://www.securityweek.com/yahoo-discloses-netiq-imanager-flaws-allowing-remote-code-execution/

Vulnerabilidad crítica en Microsoft SharePoint permite ejecución remota de código

Investigadores de Rapid7 han revelado que la vulnerabilidad CVE-2024-38094 en Microsoft SharePoint está siendo activamente explotada para comprometer redes corporativas. Esta falla permite la ejecución remota de código en servidores SharePoint no actualizados, lo que facilita que los atacantes obtengan control total de la red afectada. Una vez comprometido, el atacante puede moverse lateralmente y operar sin ser detectado durante un tiempo prolongado, poniendo en riesgo la integridad y seguridad de los datos corporativos.

Para mitigar estos ataques, se recomienda a las organizaciones aplicar inmediatamente las actualizaciones de seguridad lanzadas por Microsoft en julio de 2024. Además, es crucial revisar las configuraciones de seguridad de los servidores SharePoint, implementar sistemas de detección de intrusiones, y monitorear la actividad de la red para identificar cualquier comportamiento inusual que pudiera indicar un intento de explotación. Estas medidas ayudarán a proteger la infraestructura crítica contra accesos no autorizados.

Prioridad: Crítico

Ampliar información:

https://www.bleepingcomputer.com/news/security/microsoft-sharepoint-rce-bug-exploited-to-breach-corporate-network/

Herramienta de IA de Google descubre vulnerabilidad de día cero en SQLite

El equipo de Google ha descubierto una vulnerabilidad de día cero en SQLite utilizando su marco basado en inteligencia artificial, Big Sleep. La vulnerabilidad, identificada como CVE-2024-12345, es un subdesbordamiento de búfer en la pila, que permite a los atacantes ejecutar código arbitrario o provocar fallos en el sistema al acceder a ubicaciones de memoria antes del inicio del búfer. Este problema representa un riesgo crítico para sistemas que utilizan esta biblioteca ampliamente integrada.

Después de la divulgación responsable, los desarrolladores de SQLite corrigieron la vulnerabilidad a principios de octubre de 2024. Se aconseja a todos los desarrolladores y usuarios que actualicen a la versión más reciente de SQLite para evitar posibles ataques y que revisen sus sistemas para confirmar que no se están utilizando versiones afectadas. Mantener las implementaciones actualizadas es crucial para proteger la infraestructura de posibles explotaciones.

Prioridad: Crítico.

Ampliar información:

https://thehackernews.com/2024/11/googles-ai-tool-big-sleep-finds-zero.html

---

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 contribuir a fortalecer la seguridad de los sistemas.

MALWARE

Malware "Pygmy Goat" utilizado en ataque a cortafuegos Sophos en red gubernamental

El Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC) ha revelado que actores de amenazas han utilizado un malware personalizado llamado "Pygmy Goat" para comprometer dispositivos Sophos XG Firewall en una red gubernamental. El ataque se llevó a cabo explotando la vulnerabilidad CVE-2022-1040, que permite a los atacantes obtener acceso no autorizado y persistente. El malware se propaga a través de esta vulnerabilidad y utiliza técnicas avanzadas para mantenerse oculto y operar sin ser detectado.

El "Pygmy Goat" es un rootkit diseñado para imitar archivos legítimos de Sophos, lo que le permite evadir las medidas de detección tradicionales. Como respuesta, se recomienda a las organizaciones actualizar sus dispositivos Sophos XG Firewall con los últimos parches de seguridad, revisar las configuraciones de seguridad y monitorear la red en busca de

comportamientos anómalos. Estas acciones son esenciales para prevenir el acceso no autorizado y proteger la integridad de las redes afectadas.

Prioridad: Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/custom-pygmy-goat-malware-used-in-sophos-firewall-hack-on-govt-network/

Nueva variante del malware FakeCall secuestra dispositivos Android para llamadas fraudulentas

Investigadores de Zimperium han descubierto una nueva variante del malware FakeCall que se dirige a usuarios de Android. Este malware se propaga mediante aplicaciones maliciosas que se hacen pasar por servicios financieros legítimos. Una vez que la víctima descarga la aplicación y le concede permisos de accesibilidad, el malware obtiene control total del dispositivo. FakeCall intercepta y redirige las llamadas telefónicas, permitiendo a los atacantes hacerse pasar por representantes de bancos y engañar a las víctimas para que entreguen información confidencial.

Para protegerse de esta amenaza, los expertos recomiendan descargar aplicaciones únicamente desde tiendas oficiales como Google Play, verificar cuidadosamente los permisos solicitados por las aplicaciones y mantener el software del dispositivo actualizado. También es fundamental usar herramientas de seguridad móvil que puedan detectar y bloquear actividades sospechosas. La precaución, así como la seguridad digital son claves para prevenir ataques de este tipo.

Prioridad: Importante.

Ampliar información:

https://thehackernews.com/2024/11/new-fakecall-malware-variant-hijacks.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.

NOTICIAS DE CIBERSEGURIDAD

Fuga masiva de configuración de git expone repositorios y credenciales privadas

Una vulnerabilidad en archivos de configuración. git/config expuso al menos 15,000 repositorios y credenciales, permitiendo el acceso a sistemas críticos y servicios en la nube. La firma Sysdig descubrió la brecha, bautizada como "EMERALDWHALE," en la que se clonaron más de 10,000 repositorios privados, almacenando estos datos en un servidor vulnerable que Amazon luego eliminó.

Se recomienda a los desarrolladores proteger sus repositorios verificando la configuración de seguridad, evitando almacenar credenciales en archivos sensibles y aplicando autenticación multifactor para prevenir accesos no autorizados.

Prioridad: Importante.

Ampliar información:

https://thehackernews.com/2024/11/massive-git-config-breach-exposes-15000.html

---

Amenazas cibernéticas que podrían afectar al sector minorista esta temporada navideña

Imperva, una destacada empresa de ciberseguridad, ha advertido sobre el aumento de ataques cibernéticos dirigidos al sector minorista durante la temporada navideña. Según el informe, los sitios de comercio electrónico están enfrentando un promedio de 569,884 ataques diarios impulsados por inteligencia artificial, siendo la explotación de la lógica empresarial la amenaza más frecuente (30.7%). Estos ataques manipulan funciones legítimas de las aplicaciones para obtener ventajas no autorizadas, como el abuso de promociones o políticas de devolución.

Para mitigar estas amenazas, se recomienda a los minoristas implementar medidas de seguridad que monitoreen y validen las acciones de los usuarios en tiempo real. Además, es crucial invertir en soluciones para mitigar ataques DDoS, que han aumentado en un 61% desde el año pasado, y protegerse contra bots maliciosos, que representan el 20.8% de las amenazas. Estas precauciones son esenciales para proteger las operaciones en línea y garantizar una experiencia segura para los compradores durante esta temporada crítica.

Prioridad: Importante.

Ampliar información:

https://thehackernews.com/2024/11/cyber-threats-that-could-impact-retail.html