GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0125

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

VULNERABILIDADES

Vulnerabilidad crítica en LDAP de Windows permite ataques de Denegación de Servicio (CVE-2024-49113)

Investigadores han identificado una nueva vulnerabilidad en el protocolo LDAP de Windows, conocida como LDAPNightmare (CVE-2024-49113), con una puntuación CVSS de 7,5. Este exploit permite a atacantes remotos provocar bloqueos y reinicios en servidores Windows sin parchear, incluidos aquellos que no son controladores de dominio. Descubierta por Yuki Chen y revelada el 10 de diciembre de 2024, esta falla de denegación de servicio utiliza paquetes diseñados para manipular solicitudes DNS y LDAP, causando fallos en el proceso LSASS. SafeBreach Labs ha desarrollado un exploit de prueba de concepto que demuestra

el impacto potencial de este ataque en servidores expuestos. Microsoft ya ha emitido parches para mitigar esta vulnerabilidad crítica.

Prioridad: Crítico

Ampliar información:

https://securityaffairs.com/172618/security/ldapnightmare-exploit-cve-2024-49113.html

---

Vulnerabilidad crítica de escalada de privilegios en el registro de Windows (CVE-2024-43452)

Investigadores han publicado un exploit de prueba de concepto (PoC) para CVE-2024-43452, una vulnerabilidad crítica que permite a atacantes elevar privilegios en sistemas Windows comprometidos, otorgándoles acceso no autorizado a datos confidenciales y recursos críticos. La falla reside en la gestión de claves del registro de Windows, específicamente aquellas que requieren privilegios administrativos para ser modificadas. El exploit PoC demuestra cómo un atacante puede manipular estas claves para obtener derechos administrativos, facilitando actividades maliciosas sin interacción del usuario. Se recomienda aplicar parches de seguridad, implementar monitoreo de registros, auditar configuraciones y limitar privilegios de usuarios para mitigar los riesgos.

Prioridad: Crítico

Ampliar información:

https://gbhackers.com/windows-registry-privilege-escalation-vulnerability/

Vulnerabilidad en Nuclei permite ejecución de código arbitrario

Una vulnerabilidad crítica en el escáner de vulnerabilidades Nuclei, identificada como CVE-2024-43405 (CVSS 7.8), permitió a atacantes ejecutar código arbitrario mediante plantillas

maliciosas. Este defecto, presente en las versiones 3.0.0 a 3.3.1, se origina en discrepancias en la verificación de firmas de las plantillas y su análisis YAML. Los atacantes podían inyectar contenido ejecutable no verificado en plantillas aparentemente benignas, comprometiendo sistemas o exfiltrando datos en plataformas de escaneo automatizado.

Para mitigar este riesgo, las organizaciones deben actualizar Nuclei a la versión 3.3.2 o superior. Además, se recomienda ejecutar el escáner en entornos aislados y validar rigurosamente las plantillas utilizadas, especialmente aquellas provenientes de fuentes no confiables o de la comunidad.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/code-execution-flaw-found-in-nuclei-vulnerability-scanner/

Recomendaciones generales sobre vulnerabilidades:

- Actualizar todos los servidores Windows con los últimos parches de seguridad proporcionados por Microsoft en la actualización de diciembre de 2024. Este parche corrige la vulnerabilidad y mitiga el riesgo de explotación.
- Restringir el acceso al puerto LDAP/CLDAP (puerto 389) en entornos que no lo requieran explícitamente. Implementar listas de control de acceso (ACL) en los firewalls para limitar las conexiones solo a fuentes confiables.
- Monitorizar los registros de actividad LDAP y DNS en busca de comportamientos anómalos. Establecer alertas para detectar patrones sospechosos que puedan indicar intentos de explotación.

- Aplicar de inmediato las actualizaciones de seguridad disponibles para corregir esta vulnerabilidad crítica con una puntuación CVSS de 9.8. Ignorar estas actualizaciones puede exponer los sistemas a riesgos significativos.
- Desactivar funciones innecesarias en servidores LDAP y limitar las solicitudes de clientes desconocidos. Configurar políticas de seguridad que reduzcan la superficie de ataque de los servicios expuestos.
- Realizar pruebas de penetración regulares para evaluar la exposición de los servidores LDAP y fortalecer su configuración. Implementar medidas proactivas para evitar posibles vulnerabilidades futuras.
- Actualizar a la versión 3.3.2 de Nuclei o superior para garantizar que la vulnerabilidad esté corregida y reducir el riesgo de explotación por parte de atacantes.
- Validar rigurosamente todas las plantillas antes de ejecutarlas, especialmente aquellas provenientes de fuentes no confiables o de la comunidad. Realizar revisiones manuales y automatizadas para detectar posibles inyecciones maliciosas.

MALWARE

Nuevo malware FireScam se disfraza de Telegram Premium para robar datos en Android

Una nueva amenaza para dispositivos Android, llamada "FireScam", está disfrazada como una falsa aplicación de Telegram Premium y es capaz de robar información personal de las víctimas. Este malware se esconde en aplicaciones legítimas utilizando plataformas como Firebase, lo que le permite evadir la detección y recopilar datos confidenciales de las víctimas, como mensajes y notificaciones.

La infección comienza a través de un sitio de phishing alojado en GitHub, que se presenta como la tienda de aplicaciones RuStore, distribuyendo la versión maliciosa de Telegram

Premium. Una vez instalado, FireScam puede seguir comunicándose con los atacantes, almacenar datos robados y actualizarse con más malware.

Este tipo de ataque resalta la creciente sofisticación del malware dirigido a dispositivos Android y demuestra cómo los atacantes utilizan aplicaciones populares y servicios legítimos para engañar a los usuarios y mantener el control sobre sus dispositivos comprometidos.

Prioridad: Urgente

Ampliar información:

https://www.darkreading.com/cyberattacks-data-breaches/firescam-android-spyware-campaign-significant-threat-worldwide

---

Scripts de Python funcionan como canal para la distribución del malware SwaetRAT

Un script de Python está siendo utilizado para distribuir un nuevo malware llamado SwaetRAT. Este script interactúa directamente con el sistema operativo Windows, lo que le permite modificar configuraciones evadiendo, además, medidas de seguridad. A través de un proceso complejo, el script puede cargar y ejecutar código malicioso que se oculta y se replica en el sistema.

El malware se camufla y se copia en varias ubicaciones dentro del sistema, lo que le permite mantener su persistencia. También tiene la capacidad de extraer y ejecutar comandos maliciosos de forma remota, convirtiéndose en una herramienta peligrosa para los atacantes.

Prioridad: Importante

Ampliar información:

https://gbhackers.com/swaetrat-python-malware/

Recomendaciones generales sobre malware:

Es fundamental tener siempre actualizado el software de seguridad en tu dispositivo, como antivirus y programas de detección de amenazas. Además, evitar descargar o ejecutar programas que provengan de fuentes no confiables. Si se tienen dudas sobre una aplicación, es importante asegurarse de que provenga de tiendas oficiales como Google Play. También es útil revisar regularmente los dispositivos en busca de comportamientos inusuales y mantener una vigilancia constante de las conexiones de red. Educar a los usuarios para que reconozcan los intentos de engaño, como correos electrónicos o enlaces sospechosos, es crucial para prevenir la infección.

Nunca descargar aplicaciones de fuentes desconocidas o sitios web sospechosos, ya que pueden estar ocultando malware. Mantener siempre su dispositivo actualizado con los últimos parches de seguridad. Si se sospecha que el dispositivo puede estar infectado, es importante realizar un análisis de seguridad con una aplicación confiable. También es recomendable tener precaución al hacer clic en enlaces o correos electrónicos desconocidos.

NOTICIAS DE CIBERSEGURIDAD

Vulnerabilidad crítica en UpdraftPlus expone a más de 3 millones de sitios WordPress a riesgos

Se ha descubierto una vulnerabilidad crítica en el complemento UpdraftPlus: WP Backup & Migration, que afecta a más de 3 millones de sitios web de WordPress. Esta falla de seguridad, identificada como CVE-2024-10957, permite la inyección de objetos PHP a través

de la deserialización de entradas no confiables, lo que puede ser explotado por atacantes no autenticados.

La vulnerabilidad afecta a todas las versiones del complemento hasta la 1.24.11 inclusive. El riesgo ha sido solucionado en la versión 1.24.12, por lo que se recomienda encarecidamente a los administradores de sitios web actualizar el complemento a la última versión disponible.

Este problema de alta gravedad, con una puntuación CVSS de 8.8, podría tener consecuencias graves como la eliminación no autorizada de archivos, el robo de datos confidenciales o la ejecución remota de código. La explotación de esta vulnerabilidad se activa cuando un administrador realiza una búsqueda y reemplazo en el complemento.

Los propietarios de sitios que utilizan UpdraftPlus deben actualizar el complemento de inmediato y revisar todos los componentes de sus instalaciones de WordPress para asegurar que estén protegidos contra posibles ataques.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/wordpress-plugin-vulnerability/

Más empresas de telecomunicaciones de EE. UU. víctimas de los ciberataques de Salt Typhoon

Un grupo de amenazas respaldado por el estado chino, conocido como Salt Typhoon, ha ampliado su alcance en una ola de infracciones cibernéticas dirigidas a empresas de telecomunicaciones en los Estados Unidos. Recientemente, AT&T, Verizon y Lumen confirmaron que habían expulsado a los piratas informáticos de sus redes tras acceder a información sensible, como mensajes de texto, llamadas telefónicas y detalles sobre escuchas telefónicas de personas investigadas. También T-Mobile reveló en noviembre

que atacantes desconocidos comprometieron algunos de sus enrutadores, aunque no se vinculó este ataque directamente con Salt Typhoon.

Durante el fin de semana, fuentes del Wall Street Journal indicaron que los piratas informáticos también habían atacado Charter Communications, Consolidated Communications y Windstream, aunque estas empresas no confirmaron oficialmente los incidentes. La CISA, agencia de ciberseguridad, recomendó el uso de aplicaciones de mensajería cifradas como Signal para proteger las comunicaciones y publicó una guía para reforzar los sistemas contra estos ataques. Además, el gobierno de EE. UU. planea tomar medidas enérgicas contra China Telecom y otros riesgos relacionados con el uso de equipos vulnerables en estos ciberataques.

Prioridad: Importante

Ampliar información:

https://www.bleepingcomputer.com/news/security/charter-and-windstream-among-nine-us-telecoms-hacked-by-china/

Malware Wallet Drainer utilizado para robar 500 millones de dólares en criptomonedas en 2024

En 2024, el malware causó pérdidas de casi 500 millones de dólares, afectando a más de 332.000 víctimas. Estos ataques engañan a las personas para que firmen transacciones maliciosas, resultando en el robo de criptomonedas. Las pérdidas fueron un 67% mayores que en el año anterior, con el robo individual más grande alcanzando los 55.48 millones de dólares. La mayoría de los ataques ocurrieron en el primer trimestre, con 175.000 víctimas y pérdidas de 187.2 millones de dólares.

Los datos de Scam Sniffer indican que hubo 30 incidentes que resultaron en pérdidas superiores a un millón de dólares, con un total de 171 millones de dólares. Aunque los

ataques fueron más frecuentes a principios de año, los mayores robos ocurrieron en agosto y septiembre. A pesar de un descenso en la actividad hacia la segunda mitad de 2024, el robo de criptomonedas en general aumentó, con más de 2.200 millones de dólares sustraídos, según Chainalysis.

Prioridad: Importante

Ampliar información:

https://www.securityweek.com/wallet-drainer-malware-used-to-steal-500-million-in-cryptocurrency-in-2024/
