GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1625

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

VULNERABILIDADES

Alerta en Windows: vulnerabilidad NTLM (CVE-2025-24054) explotada para robo de hashes

Una nueva vulnerabilidad en Microsoft Windows está siendo explotada activamente para robar credenciales. Identificada como CVE-2025-24054, esta falla de suplantación de identidad (spoofing) afecta al protocolo NTLM (New Technology LAN Manager), permitiendo la exfiltración de hashes NTLMv2-SSP sin necesidad de que el usuario ejecute archivos maliciosos.

La vulnerabilidad reside en un fallo de validación de rutas en archivos. library-ms (CWE-73), y permite a atacantes no autenticados desencadenar solicitudes SMB desde el explorador de Windows hacia servidores controlados, simplemente tras descargar y descomprimir archivos .zip maliciosos —o incluso sin compresión—. Reportes de Check Point Research confirman campañas activas de malspam que utilizan este vector, dirigidas

a entidades en Polonia y Rumania, y lo vinculan con tácticas usadas por grupos como UAC-0194 y Blind Eagle.

A pesar de haber sido parcheada en el Patch Tuesday de marzo, su explotación activa ha llevado a CISA (Agencia de Ciberseguridad de EE.UU.) a incluirla en el catálogo de vulnerabilidades activamente explotadas, exigiendo a las agencias federales aplicar el parche antes del 8 de mayo de 2025.

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-24054 (Variante de CVE-2024-43451, usado previamente en ataques dirigidos)

Recomendaciones de mitigación:

- Deshabilitar NTLM mediante políticas de grupo y favorecer Kerberos.
- Bloquear tráfico SMB saliente no autorizado en firewalls.
- Monitorizar conexiones SMB hacia dominios externos.
- Capacitar a usuarios sobre los riesgos de archivos. library-ms y archivos comprimidos de fuentes desconocidas.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2025/04/cve-2025-24054-under-active.html
- https://vulners.com/thn/THN:95C876E2AE4F101CE2B1FC68D68915AE
- https://research.checkpoint.com/2025/cve-2025-24054-ntlm-exploit-in-the-wild/

Vulnerabilidad crítica en Windows Remote Desktop Gateway (CVE-2025-27480)

Microsoft ha identificado y corregido la vulnerabilidad CVE-2025-27480, una falla de tipo *use-after-free* en el servicio Remote Desktop Gateway (RD Gateway) de Windows. Esta vulnerabilidad permite a un atacante remoto no autenticado ejecutar código arbitrario en

sistemas afectados, comprometiendo la confidencialidad, integridad y disponibilidad del sistema.

La explotación de esta vulnerabilidad requiere que el atacante gane una condición de carrera (*race condition*), lo que implica una alta complejidad en el ataque. Sin embargo, debido a la gravedad del impacto y la posibilidad de explotación remota sin autenticación, Microsoft ha clasificado esta vulnerabilidad como crítica y ha indicado que la explotación es "más probable".

Los sistemas afectados incluyen versiones de Windows Server que tienen habilitado el rol de RD Gateway. Se han lanzado actualizaciones de seguridad para mitigar esta vulnerabilidad en las siguientes versiones:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Detalles técnicos:

- CVE: CVE-2025-27480
- Tipo: Ejecución remota de código (RCE)
- Componente afectado: Windows Remote Desktop Gateway Service
- Vector de ataque: Remoto, sin autenticación
- Complejidad del ataque: Alta (requiere ganar una condición de carrera)
- Interacción del usuario: No requerida
- Impacto: Compromiso total del sistema

Prioridad: Urgente.

Ampliar Información:

https://www.tenable.com/cve/CVE-2025-27480

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27480

Vulnerabilidad crítica en Windows CLFS (CVE-2025-29824) Exploited en campañas de ransomware

Microsoft ha identificado y corregido la vulnerabilidad CVE-2025-29824, una falla de tipo use-after-free en el controlador del Common Log File System (CLFS) de Windows. Esta vulnerabilidad permite a un atacante local elevar sus privilegios al nivel de SYSTEM, otorgándole control total sobre el sistema afectado.

La explotación activa de esta vulnerabilidad ha sido vinculada a campañas de ransomware, donde el grupo de amenazas Storm-2460 ha utilizado el malware PipeMagic para desplegar cargas maliciosas en sistemas comprometidos.

Aunque Microsoft ha lanzado parches para mitigar esta amenaza, es importante destacar que algunas versiones de Windows 10 (32 y 64 bits) aún no han recibido actualizaciones, dejando a estos sistemas expuestos a posibles ataques.

Detalles técnicos:

- CVE: CVE-2025-29824
- Tipo: Elevación de privilegios (EoP)
- Componente afectado: Windows CLFS Driver
- Vector de ataque: Local (requiere acceso al sistema)
- Estado: Explotación activa confirmada
- Parche disponible: Sí, excepto para ciertas versiones de Windows 10

Recomendaciones de mitigación:

- Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Server.
- Restringir el acceso al servicio RD Gateway mediante listas de control de acceso (ACL) y firewalls, permitiendo solo conexiones desde direcciones IP confiables.
- Monitorear los sistemas en busca de actividades sospechosas o inusuales relacionadas con el servicio RD Gateway.

Prioridad: Urgente.

Ampliar Información:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Serve
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Alerta: malware en Docker explota nodos Teneo Web3 para generar criptomonedas mediante señales falsas

Investigadores de ciberseguridad han identificado una campaña maliciosa que apunta a entornos Docker, utilizando una técnica no documentada previamente para obtener ganancias ilícitas en criptomonedas. El ataque se centra en Teneo, un servicio Web3 descentralizado que permite a los usuarios monetizar datos de redes sociales ejecutando un nodo comunitario.

El malware despliega un contenedor Docker desde la imagen "kazutod/tene: ten" alojada en Docker Hub, la cual contiene un script en Python altamente ofuscado. Este script establece una conexión con el servicio de Teneo y envía señales de "keep-alive" o "heartbeat" falsas, simulando actividad legítima para acumular puntos que pueden convertirse en tokens $TENEO.

A diferencia de ataques tradicionales de cryptojacking que utilizan herramientas como XMRig para minar criptomonedas directamente, esta campaña se basa en la explotación de la infraestructura de Teneo para obtener recompensas, evitando así mecanismos de detección comunes.

Recomendaciones para mitigar el riesgo:

- Restringir el acceso al API de Docker: Asegurar que el API de Docker no esté expuesto públicamente y esté protegido por autenticación adecuada.
- Monitorear imágenes de contenedores: Verificar la procedencia y el contenido de las imágenes antes de su despliegue, evitando aquellas de fuentes no confiables.
- Implementar políticas de seguridad en Docker: Utilizar herramientas y configuraciones que limiten las capacidades de los contenedores, reduciendo el riesgo de ejecución de código malicioso.
- Actualizar regularmente: Mantener Docker y sus componentes actualizados para corregir posibles vulnerabilidades conocidas.

- Educar al personal: Capacitar a los equipos de desarrollo y operaciones sobre las mejores prácticas de seguridad en entornos de contenedores.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/04/docker-malware-exploits-teneo-web3-node.html

---

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Extensiones de Chrome bajo ataque: “Cookie Bite” permiten el robo de sesiones activas sin contraseña

Investigadores de ciberseguridad han documentado un nuevo vector de ataque denominado Cookie Bite, que demuestra cómo extensiones maliciosas en Google Chrome

pueden ser utilizadas para robar tokens de sesión y cookies de autenticación, permitiendo a los atacantes secuestrar cuentas sin necesidad de credenciales.

La prueba de concepto, publicada por investigadores independientes, muestra cómo una extensión aparentemente legítima puede acceder a las cookies activas de sesión de sitios web como Google, Microsoft, y servicios con autenticación multifactor (MFA) como LastPass y Aegis Authenticator. Una vez robadas, las cookies pueden ser exportadas a un servidor controlado por el atacante y reutilizadas para acceder a las cuentas objetivo, sin necesidad de autenticarse nuevamente.

Lo preocupante es que este ataque no explota una vulnerabilidad del navegador en sí, sino un uso abusivo de los permisos legítimos que muchas extensiones solicitan y que los usuarios suelen conceder sin revisar cuidadosamente. Esta técnica evade protecciones como la encriptación de cookies de Chrome, ya que el acceso ocurre antes de que esa encriptación entre en juego.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/cookie-bite-attack-poc-uses-chrome-extension-to-steal-session-tokens/

Alerta de Seguridad: grupos APT adoptan la técnica de ingeniería social “ClickFix” para comprometer sistemas

Investigadores de ciberseguridad han identificado que múltiples grupos de amenazas persistentes avanzadas (APT) respaldados por estados-nación, incluyendo a Kimsuky (Corea del Norte), MuddyWater (Irán), APT28 y UNK_RemoteRogue (Rusia), están utilizando una táctica de ingeniería social conocida como ClickFix en campañas de espionaje dirigidas.

ClickFix es una técnica que implica la creación de sitios web maliciosos que simulan ser plataformas legítimas de software o intercambio de documentos. A través de correos electrónicos de phishing o publicidad maliciosa, las víctimas son dirigidas a estos sitios donde se les presentan mensajes de error falsos indicando fallos en la descarga o visualización de documentos. Posteriormente, se les solicita hacer clic en un botón de "Reparar", que les instruye a ejecutar scripts de PowerShell o comandos de línea de comandos, lo que conduce a la ejecución de malware en sus dispositivos.

Esta táctica ha sido observada en campañas recientes, incluyendo una donde el actor estatal norcoreano 'Kimsuky' utilizó una página web falsa de "registro de dispositivo" como parte de su estrategia de ataque.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/new-clickfix-attack-deploys-havoc-c2-via-microsoft-sharepoint/

https://www.bleepingcomputer.com/news/security/state-sponsored-hackers-embrace-clickfix-social-engineering-tactic