GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3825

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	0	1
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

VULNERABILIDADES CRÍTICAS EN CHAOS MESH (CHAOTIC DEPUTY – CVE-2025-59358/59/60/61)

El 16 de septiembre de 2025, investigadores de JFrog revelaron múltiples vulnerabilidades críticas en Chaos Mesh, la plataforma de Chaos Engineering para Kubernetes. Las fallas, agrupadas bajo el nombre “Chaotic Deputy”, permiten la ejecución remota de código (RCE) y la toma de control total del clúster Kubernetes, incluso en configuraciones por defecto.

Resumen técnico:

- **CVE-2025-59358 (CVSS 7.5):** el Controller Manager expone un servidor GraphQL de depuración sin autenticación en el puerto 10082. Esto habilita un atacante dentro del clúster a ejecutar fault injections arbitrarios (ej. matar procesos en cualquier pod), provocando un DoS a nivel de clúster.

- **CVE-2025-59359 (CVSS 9.8):** vulnerabilidad de command injection en la mutación cleanTcs.
- **CVE-2025-59360 (CVSS 9.8):** vulnerabilidad de command injection en la mutación killProcesses.
- **CVE-2025-59361 (CVSS 9.8):** vulnerabilidad de command injection en la mutación cleanIptables.
- Un atacante con acceso a la red interna del clúster puede encadenar estas fallas para ejecutar comandos arbitrarios en cualquier pod, robar tokens de cuentas de servicio privilegiadas desde: **/proc/<pid>/root/var/run/secrets/kubernetes.io/serviceaccount/token** y escalar privilegios hasta controlar todo el clúster.

Impacto potencial:

- Toma completa de clústeres Kubernetes que ejecuten Chaos Mesh vulnerable.
- Robo de credenciales y datos sensibles desde pods comprometidos.
- Movimientos laterales y persistencia mediante abuso de cuentas de servicio.
- Riesgo elevado en infraestructuras críticas que usan Azure Chaos Studio y otros servicios que integran Chaos Mesh.

Recomendaciones de mitigación:

1. Actualizar de inmediato a Chaos Mesh 2.7.3 o superior (liberado el 21 de agosto de 2025).
2. Si no es posible actualizar, deshabilitar el servidor de control (**enableCtrlServer=false**) al redeplegar con Helm Chart.
3. Restringir el acceso a la red hacia el puerto 10082 y aplicar políticas RBAC más estrictas.
4. Monitorizar actividad en logs de kubectl y SIEM en busca de accesos anómalos o intentos de inyección.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/09/chaos-mesh-critical-graphql-flaws.html
- https://unaaldia.hispasec.com/2025/09/vulnerabilidades-criticas-en-chaos-mesh-permiten-la-toma-total-de-clusteres-kubernetes.html
- https://jfrog.com/blog/chaotic-deputy-critical-vulnerabilities-in-chaos-mesh-lead-to-kubernetes-cluster-takeover/

VULNERABILIDAD CRÍTICA EN SAMSUNG ANDROID (CVE-2025-21043 – ZERO-DAY)

El 12 de septiembre de 2025, Samsung publicó su boletín mensual de seguridad para Android, corrigiendo una vulnerabilidad crítica que estaba siendo explotada activamente en ataques dirigidos contra dispositivos móviles.

Resumen técnico:

- **CVE-2025-21043 (CVSS 8.8):** vulnerabilidad de tipo out-of-bounds write en la librería cerrada libimagecodec.quram.so, desarrollada por Quramsoft.
- Afecta a dispositivos Samsung con Android 13, 14, 15 y 16.
- La explotación permite la ejecución remota de código (RCE) a través de imágenes especialmente diseñadas.
- Samsung confirmó la existencia de exploits en la naturaleza, aunque no compartió detalles sobre los actores detrás de la campaña.

Impacto potencial:

- Compromiso total de dispositivos Samsung Android vulnerables.
- Ejecución de código malicioso mediante imágenes cargadas en apps o navegadores.
- Posible escalada de privilegios y robo de información sensible (mensajes, credenciales, datos financieros).
- Riesgo elevado en entornos corporativos con dispositivos BYOD sin parchear.

Recomendaciones de mitigación:

1. Actualizar inmediatamente los dispositivos afectados al Samsung Security Maintenance Release (SMR) – septiembre 2025, Release 1.
2. Evitar la apertura de archivos e imágenes de fuentes no confiables hasta haber aplicado el parche.
3. Implementar soluciones de gestión de dispositivos móviles (MDM/MAM) para validar versiones de firmware en entornos corporativos.
4. Monitorear comportamientos anómalos en dispositivos móviles, especialmente en aplicaciones que procesan imágenes.

Prioridad: Crítica

Ampliar Información:

- https://thehackernews.com/2025/09/samsung-fixes-critical-zero-day-cve.html
- https://cibernoticias.blog/2025/09/13/samsung-cve-2025-21043-vulnerabilidad/
- https://unaaldia.hispasec.com/2025/09/samsung-corrige-vulnerabilidad-critica-cve-2025-21043-explotada-activamente-en-android.html

VULNERABILIDADES CRÍTICAS EN MICROSOFT (PATCH TUESDAY – SEPTIEMBRE 2025)

El 10 de septiembre de 2025, Microsoft publicó actualizaciones de seguridad que corrigen 80 vulnerabilidades en sus productos, de las cuales 8 son críticas y 72 importantes. Ninguna estaba siendo explotada activamente al momento del lanzamiento, aunque una de ellas había sido divulgada públicamente.

Resumen técnico:

- **CVE-2025-55234 (CVSS 8.8 – SMB, divulgada públicamente):** vulnerabilidad de elevación de privilegios en el servidor SMB. Permite ataques de relay si no están habilitados mecanismos de endurecimiento como SMB Signing y Extended Protection for Authentication (EPA), facilitando movimiento lateral y robo de credenciales.
- **CVE-2025-54914 (CVSS 10.0 – Azure Networking):** vulnerabilidad crítica de elevación de privilegios en Azure. No requiere acción por parte de clientes, ya mitigada por Microsoft en la nube.
- **CVE-2025-55232 (CVSS 9.8 – Microsoft HPC Pack):** vulnerabilidad de ejecución remota de código (RCE) al enviar paquetes maliciosos que otorgan privilegios de sistema.
- **CVE-2025-54918 (CVSS 8.8 – Windows NTLM):** falla de autenticación NTLM que permite a un atacante con credenciales válidas o hashes ejecutar escaladas a SYSTEM.
- **CVE-2025-54911 y CVE-2025-54912 (BitLocker EoP, CVSS 7.3/7.8):** continúan la serie de fallas en BitLocker ("BitUnlocker"), que permiten evadir protecciones de cifrado en escenarios de acceso físico.

Además, se corrigieron vulnerabilidades en Microsoft Office (Word, Excel, PowerPoint, Visio, SharePoint), Hyper-V, NTFS, RRAS, SQL Server y el navegador Edge.

Impacto potencial:

- Compromiso total de sistemas Windows mediante escaladas de privilegios locales o remotas.
- Riesgo de relay attacks y robo de credenciales vía SMB.
- Explotación en entornos de nube (Azure) y de cómputo de alto rendimiento (HPC).
- Riesgo para la protección de datos cifrados con BitLocker en escenarios de pérdida o robo de equipos.

Recomendaciones de mitigación:

1. Aplicar de inmediato las actualizaciones liberadas en el Patch Tuesday de septiembre 2025.
2. Habilitar auditoría de compatibilidad SMB y aplicar SMB Signing + EPA en servidores Windows.
3. Endurecer configuraciones de NTLM y minimizar su uso en redes corporativas.
4. Activar TPM+PIN en BitLocker para proteger datos frente a ataques con acceso físico.
5. Validar compatibilidad de aplicaciones y entornos antes de aplicar mitigaciones avanzadas.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2025/09/microsoft-fixes-80-flaws-including-smb.html
- https://its.hku.hk/security-alerts/microsoft-fixes-80-flaws-including-smb-privesc-and-azure-cvss-10-0-bugs/
- https://app.daily.dev/posts/microsoft-fixes-80-flaws-including-smb-privesc-and-azure-cvss-10-0-bugs-ns0eezgat

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 Server
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

EGGSTREME: FRAMEWORK FILELESS ATRIBUIDO A APT CHINO

El 10 de septiembre de 2025, investigadores de Bitdefender revelaron una nueva campaña atribuida a un grupo APT chino contra una empresa militar en Filipinas, mediante un framework de malware fileless denominado EggStreme.

Resumen técnico:

- EggStreme se despliega en múltiples etapas:
- EggStremeFuel (mscorsvc.dll) – carga inicial vía DLL sideloading que abre canal de C2 y entrega EggStremeLoader.
- EggStremeReflectiveLoader – carga en memoria del payload final.

- EggStremeAgent – backdoor principal con 58 comandos: reconocimiento, escalada de privilegios, movimiento lateral, keylogger, ejecución de shellcode y exfiltración.
- EggStremeWizard – backdoor secundario con reverse shell y capacidades de transferencia de archivos.
- El framework opera directamente en memoria (fileless), evadiendo soluciones basadas en disco.
- Se observó uso de gRPC para comunicaciones C2 y Stowaway proxy para pivotar dentro de la red.
- Persistencia conseguida abusando de servicios legítimos de Windows deshabilitados por defecto.

Impacto potencial:

- Acceso persistente y sigiloso en redes comprometidas.
- Robo de credenciales y datos sensibles de alto valor estratégico.
- Potencial de espionaje a largo plazo en objetivos militares y gubernamentales.
- Difícil detección por la naturaleza fileless y el abuso de binarios legítimos.

Recomendaciones de mitigación:

1. Restringir binarios de alto riesgo (ej. xwizard.exe, WinMail.exe) para reducir superficie de ataque.
2. Implementar detección y respuesta (EDR/XDR) capaz de identificar patrones fileless y anomalías de comportamiento.
3. Revisar y auditar servicios deshabilitados que podrían ser abusados para persistencia.
4. Monitorear tráfico C2 inusual, incluyendo uso no autorizado de gRPC.
5. Segmentar redes críticas para limitar movimiento lateral.

Prioridad: Importante

Ampliar Información:

- https://www.infosecurity-magazine.com/news/chinese-apt-military-fileless/
- https://www.bitdefender.com/en-us/blog/businessinsights/eggstreme-fileless-malware-cyberattack-apac
- https://thehackernews.com/2025/09/chinese-apt-deploys-eggstreme-fileless.html

Recomendaciones generales sobre malware:

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

MICROSOFT Y CLOUDFLARE DESMANTELAN RACCOONO365, SERVICIO DE PHISHING MASIVO

El 17 de septiembre de 2025, Microsoft (DCU) y Cloudflare anunciaron la interrupción de RaccoonO365, una operación de Phishing-as-a-Service (PhaaS) usada para robar credenciales de Microsoft 365 a escala global.

Resumen técnico:

- Se incautaron 338 dominios y cuentas de Cloudflare Workers empleados por la infraestructura de RaccoonO365.
- El servicio, también rastreado como Storm-2246, operaba bajo modelo de suscripción: entre $355 y $999 por plan mensual/trimestral.
- Desde julio de 2024, permitió a cibercriminales robar más de 5,000 credenciales en 94 países, incluyendo campañas masivas con temática fiscal y ataques a más de 20 entidades de salud en EE.UU.
- Incorporaba técnicas avanzadas para evadir defensas:
- Uso de CAPTCHA (Cloudflare Turnstile) y detección anti-bot.
- Páginas falsas de login de Microsoft, DocuSign, Adobe y SharePoint.
- Microsoft identificó a Joshua Ogundipe (Nigeria) como líder del grupo. Una filtración de un monedero de criptomonedas facilitó la atribución.

Impacto potencial:

- Compromiso de Microsoft 365 (correo, OneDrive, SharePoint) → riesgo de extorsión, fraude financiero y ransomware posterior.
- Impacto en salud pública: retrasos en atención médica, resultados de laboratorio comprometidos, fuga de datos sensibles.

- Democratización del phishing → cualquier atacante con bajo nivel técnico podía lanzar campañas sofisticadas.

Recomendaciones para mitigar el riesgo:

- Habilitar MFA resistente a phishing (ej. FIDO2, passkeys).
- Monitorizar y bloquear dominios relacionados con RaccoonO365 y servicios similares (BulletProofLink, VoidProxy).
- Implementar defensas contra BEC y phishing masivo en Microsoft 365 (Defender for Office 365, Cloudflare Email Security, etc.).
- Educar a usuarios sobre phishing temático (impuestos, salud, documentos corporativos).
- Reforzar controles de detección de uso indebido de Cloudflare Workers y servicios legítimos.
- Sensibilizar a los empleados sobre ataques de vishing y verificar la legitimidad de cualquier solicitud de integración externa.

Prioridad: Importante.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/microsoft-and-cloudflare-disrupt-massive-raccoono365-phishing-service/
- https://thehackernews.com/2025/09/raccoono365-phishing-network-shut-down.html
- https://securityaffairs.com/182294/cyber-crime/microsoft-and-cloudflare-teamed-up-to-dismantle-the-raccoono365-phishing-service.html