GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1226

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

VULNERABILIDADES

CITRIX NETSCALER – SOBRELECTURA DE MEMORIA FUERA DE LÍMITES (CVE-2026-3055)

Citrix ha publicado una alerta de seguridad crítica para NetScaler ADC y NetScaler Gateway debido a un fallo que permite la filtración de información sensible desde la memoria del dispositivo. Esta vulnerabilidad es especialmente peligrosa ya que puede ser explotada de forma remota por atacantes no autenticados en dispositivos configurados como proveedores de identidad SAML (SAML IdP).

Resumen técnico:

- Identificador principal: CVE-2026-3055.
- Severidad: 9.3 (Crítica) en la escala CVSS v4.0.
- Causa raíz: Validación insuficiente de entradas que resulta en una sobrelectura de memoria fuera de límites (Out-of-bounds read).
- Mecanismo de falla: El componente SAML falla al procesar solicitudes maliciosas, permitiendo que un atacante lea segmentos de la memoria volátil del appliance que podrían contener secretos o datos de sesión.
- Estado de explotación: Parches publicados el 23 de marzo de 2026. Aunque no hay pruebas de concepto (PoC) públicas ni explotación activa confirmada al momento, los investigadores advierten que es inminente debido a su similitud con fallos previos como "CitrixBleed".
- Versiones afectadas: NetScaler ADC y Gateway 14.1 (antes de 14.1-66.59), 13.1 (antes de 13.1-62.23) y versiones FIPS/NDcPP (antes de 13.1-37.262).

Impacto potencial:

- Exfiltración de secretos y credenciales: La lectura de memoria puede exponer llaves criptográficas, certificados y secretos de configuración almacenados en el proceso.
- Secuestro de sesiones activas: Los atacantes podrían extraer tokens de sesión de usuarios autenticados, permitiendo el acceso a recursos corporativos sin necesidad de credenciales válidas.
- Compromiso de la infraestructura de acceso: Al ser el punto de entrada principal (SAML IdP), el compromiso de NetScaler afecta directamente a la confianza de todo el ecosistema de Single Sign-On (SSO).
- Vector para movimiento lateral: El acceso obtenido facilita a los actores de amenaza posicionarse dentro de la red perimetral para lanzar ataques contra recursos internos.

Recomendaciones de mitigación:

1. Actualización inmediata de Firmware: Migrar de forma urgente a las versiones corregidas (14.1-66.59 o 13.1-62.23 según corresponda) para cerrar el vector de ataque.
2. Auditoría de configuración SAML: Verificar si el appliance está vulnerable ejecutando el comando show authentication samlIdPProfile o buscando la cadena add authentication samlIdPProfile en el archivo de configuración.
3. Escaneo preventivo de activos: Utilizar herramientas de gestión de vulnerabilidades (ej. Qualys con QID 386883) para identificar rápidamente instancias expuestas en la infraestructura.
4. Monitoreo de logs de autenticación: Revisar patrones inusuales en las solicitudes SAML y comportamientos anómalos en el acceso de usuarios que puedan indicar un intento de explotación o secuestro de sesión.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/03/citrix-urges-patching-critical.html
- https://www.rapid7.com/blog/post/etr-cve-2026-3055-citrix-netscaler-adc-and-netscaler-gateway-out-of-bounds-read/
- https://www.securityweek.com/critical-citrix-netscaler-vulnerability-poised-for-exploitation-security-firms-warn/
- https://cibersafety.com/cve-2026-3055-cve-2026-4368-citrix-netscaler/
- https://threatprotect.qualys.com/2026/03/24/citrix-netscaler-adc-and-netscaler-gateway-multiple-vulnerabilities-cve-2026-3055-cve-2026-4368/

ORACLE IDENTITY MANAGER – EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-21992)

Oracle ha emitido un parche de emergencia (fuera de banda) para corregir una vulnerabilidad crítica en Oracle Identity Manager (OIM) y Web Services Manager. El fallo permite a un atacante remoto no autenticado ejecutar código arbitrario con privilegios elevados a través de peticiones HTTP maliciosas, lo que podría derivar en el control total de la plataforma de gobernanza de identidades.

Resumen técnico:

- Identificador principal: CVE-2026-21992.
- Severidad: 9.8 (Crítica) en la escala CVSS v3.1.
- Componentes afectados: REST WebServices (en OIM) y Web Services Security (en OWSM). Ambos forman parte de la suite Fusion Middleware.
- Mecanismo de falla: El componente afectado carece de una validación de seguridad adecuada en los endpoints de servicios web, permitiendo la inyección y ejecución de comandos sin necesidad de credenciales de usuario.
- Estado de explotación: Alerta publicada entre el 19 y 20 de marzo de 2026. Se han observado reportes de supuestos Proof-of-Concept (PoC) a la venta en foros especializados, lo que eleva significativamente el riesgo de explotación inminente.
- Versiones afectadas: Oracle Identity Manager y Web Services Manager versiones 12.2.1.4.0 y 14.1.2.1.0.

Impacto potencial:

- Toma de control total (System Takeover): El atacante puede obtener privilegios de administración sobre el servidor que aloja OIM, comprometiendo la integridad de todo el middleware.
- Compromiso de identidades corporativas: Al ser una plataforma de gobernanza, el atacante podría manipular cuentas de usuario, escalar privilegios o exfiltrar credenciales almacenadas de empleados y servicios.
- Acceso inicial y movimiento lateral: OIM suele estar expuesto o conectado a redes críticas; un compromiso aquí sirve como puente para saltar hacia el Directorio Activo u otras bases de datos sensibles.
- Interrupción de servicios críticos: La capacidad de ejecutar código permite el despliegue de ransomware o la deshabilitación de los servicios de autenticación, paralizando el acceso de los usuarios a las aplicaciones empresariales.

Recomendaciones de mitigación:

1. Aplicación inmediata del parche KB878741: Priorizar la instalación de la actualización de seguridad de emergencia proporcionada por Oracle a través de Fusion Middleware.
2. Restricción de acceso perimetral: Aislar o restringir el acceso desde redes públicas a los endpoints de administración y servicios web de OIM/OWSM, permitiendo la conexión solo desde segmentos de red confiables o mediante VPN.
3. Despliegue de reglas en WAF: Implementar firmas en el Firewall de Aplicaciones Web (WAF) que identifiquen y bloqueen peticiones HTTP POST inusuales o payloads sospechosos dirigidos a rutas de recursos /oim o /wsm.
4. Monitoreo activo de procesos: Auditar los logs del servidor de aplicaciones en busca de ejecuciones de procesos inesperados o conexiones de red salientes (outbound) anómalas originadas desde los servidores de Oracle.

Prioridad: Crítica.

Ampliar información:

- https://ciberseguridad.euskadi.eus/noticia/2026/vulnerabilidad-en-oracle-identity-manager-y-web-services-manager/webcyb00-contcibglos/es/
- https://www.oracle.com/security-alerts/alert-cve-2026-21992.html
- https://www.sophos.com/en-us/blog/oracle-vulnerability-cve-2026-21992-impacts-core-products
- https://beazley.security/alerts-advisories/critical-vulnerability-in-oracle-identity-manager-and-web-services-manager-cve-2026-21992
- https://www.securityweek.com/oracle-releases-emergency-patch-for-critical-identity-manager-vulnerability/

LANGFLOW — EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-33017)

Se ha detectado la explotación activa de una vulnerabilidad crítica en Langflow, el framework de código abierto para construir agentes de IA. El fallo permite a atacantes no autenticados ejecutar código arbitrario de Python en el servidor con una sola petición HTTP. Lo más alarmante es que los ataques comenzaron apenas 20 horas después de la divulgación del fallo, demostrando que los actores de amenaza están monitoreando de cerca las herramientas de IA debido a su acceso a datos corporativos sensibles.

Resumen técnico:

- Identificador principal: CVE-2026-33017.
- Severidad: 9.3 (Crítica) en la escala CVSS v4.0.
- Causa raíz: Falta de autenticación en un endpoint público combinada con una inyección de código (CWE-94) mediante el uso inseguro de la función exec().
- Mecanismo de falla: El endpoint /api/v1/build_public_tmp/{flow_id}/flow acepta un parámetro opcional de datos que permite al atacante inyectar definiciones de flujo con código Python malicioso. Este código se ejecuta directamente en el servidor sin ningún tipo de sandboxing o aislamiento.
- Estado de explotación: Explotación activa confirmada desde el 18 de marzo de 2026. Los atacantes han automatizado el escaneo de instancias vulnerables para exfiltrar secretos y desplegar payloads de segunda etapa.
- Versiones afectadas: Todas las versiones anteriores e incluyendo la 1.8.1.

Impacto potencial:

- Ejecución remota de código (RCE): Control total sobre el proceso del servidor de Langflow, permitiendo la ejecución de comandos con los mismos privilegios que la aplicación.
- Exfiltración masiva de llaves de API: Compromiso de variables de entorno y archivos .env que contienen credenciales críticas para servicios como OpenAI, Anthropic, AWS y bases de datos vectoriales.
- Persistencia mediante Backdoors: Los atacantes han sido observados intentando descargar scripts y herramientas adicionales para mantener el acceso a largo plazo dentro de la infraestructura.
- Compromiso de la cadena de suministro de IA: La capacidad de manipular los flujos de trabajo permite alterar la lógica de los agentes de IA, pudiendo desviar datos sensibles o inyectar respuestas maliciosas a los usuarios finales.

Recomendaciones de mitigación:

1. Actualización inmediata a la versión 1.9.0: Es imperativo migrar a la última versión disponible que elimina la posibilidad de inyectar datos de flujo a través del endpoint público afectado.
2. Rotación de secretos y credenciales: Debido a la rapidez de la explotación, se deben considerar comprometidas todas las API Keys y contraseñas de bases de datos configuradas en la instancia, procediendo a su rotación inmediata.
3. Aislamiento de red y autenticación robusta: Restringir el acceso a Langflow mediante reglas de firewall o colocarlo detrás de un proxy inverso que exija autenticación antes de permitir cualquier interacción con la API.
4. Monitoreo de tráfico y procesos: Auditar logs en busca de peticiones POST inusuales al endpoint /build_public_tmp/ y vigilar conexiones salientes hacia dominios de callback sospechosos (ej. oastify.com, interact.sh).

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/03/critical-langflow-flaw-cve-2026-33017.html
- https://ccb.belgium.be/advisories/warning-critical-vulnerability-langflow-ai-pipelines-patch-immediately
- https://www.sysdig.com/blog/cve-2026-33017-how-attackers-compromised-langflow-ai-pipelines-in-20-hours
- https://www.secpod.com/blog/cve-2026-33017-critical-langflow-vulnerability-exploited-within-20-hours-of-disclosure/
- https://www.gblock.app/articles/langflow-cve-2026-33017-ai-rce-exploit

MALWARE

GLASSWORM — CAMPAÑA DE CONTAMINACIÓN DE LA CADENA DE SUMINISTRO (MARZO 2026)

Investigadores de seguridad han alertado sobre la quinta ola de ataques de la campaña "GlassWorm", la cual utiliza caracteres Unicode invisibles para ocultar código malicioso en repositorios de código abierto. Este malware ha evolucionado hacia un framework de múltiples etapas que instala un Troyano de Acceso Remoto (RAT) persistente y una extensión maliciosa de Chrome, diseñada específicamente para comprometer el entorno de trabajo de desarrolladores y expertos en ciberseguridad.

Resumen técnico:

- Tipo de amenaza: Worm de cadena de suministro / Infostealer / RAT.
- Vector de infección: Paquetes maliciosos en npm, PyPI y Open VSX, además del compromiso de cuentas de mantenedores legítimos para realizar force-pushes en GitHub.
- Técnica de evasión principal: Uso de selectores de variación Unicode (U+FE00 a U+FE0F) que resultan invisibles en editores como VS Code, Cursor y la interfaz de GitHub, permitiendo que el payload pase desapercibido en revisiones de código manuales.
- Infraestructura C2 (Mando y Control): Utiliza la blockchain de Solana como un "punto muerto" (dead-drop). El cargador consulta los campos "memo" de transacciones en wallets específicas para obtener la URL del servidor C2, lo que hace que la infraestructura sea casi imposible de dar de baja.
- Geofencing: El malware incluye lógica para abortar la ejecución si detecta una configuración regional o zona horaria de Rusia o países de la CEI.

- Novedad de la semana: Se ha detectado la primera incursión de GlassWorm en el ecosistema de servidores MCP (Model Context Protocol), apuntando a desarrolladores que construyen herramientas de Inteligencia Artificial.

Impacto potencial:

- Exfiltración masiva de secretos de desarrollo: El malware busca activamente archivos .npmrc, tokens de GitHub, llaves SSH y variables de entorno que contienen credenciales de infraestructura crítica (AWS, GCP, Azure, Docker).
- Compromiso total de activos criptográficos: Incluye un módulo de phishing altamente sofisticado que detecta mediante WMI la conexión de hardware wallets (Ledger/Trezor) para engañar al usuario y robar la frase semilla de 24 palabras.
- Vigilancia persistente mediante RAT: El RAT basado en WebSockets permite al atacante ejecutar JavaScript arbitrario, realizar capturas de pantalla, registrar pulsaciones de teclas (keylogging) y desplegar módulos de HVNC para acceso remoto oculto.
- Envenenamiento de la cadena de suministro corporativa: Al comprometer la máquina del desarrollador, el atacante puede inyectar código malicioso en los proyectos legítimos de la empresa, propagando la infección a clientes y aliados de negocio.

Recomendaciones de mitigación:

1. Implementación de escaneo de caracteres invisibles: Utilizar herramientas de código abierto como glassworm-hunter para auditar repositorios, extensiones de VS Code y directorios node_modules en busca de clústeres de Unicode sospechosos.
2. Auditoría de extensiones de navegador: Verificar la presencia de extensiones sospechosas que suplanten a "Google Docs Offline". En entornos empresariales, se recomienda aplicar políticas de "Allowlist" para extensiones de Chrome y VS Code.
3. Rotación de tokens de infraestructura: Ante cualquier sospecha de infección, proceder con la rotación inmediata de tokens de NPM, llaves de nube y credenciales de Git, asumiendo que el volcado de memoria y variables de entorno ha sido exitoso.
4. Monitoreo de conexiones de red anómalas: Vigilar el tráfico saliente hacia RPCs de Solana o puertos inusuales asociados a C2 (ej. 45.32.150[.]251), así como el uso de protocolos WebRTC fuera de aplicaciones de comunicación autorizadas.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/03/glassworm-malware-uses-solana-dead.html
- https://afine.com/blogs/hunting-glassworm-open-source-detection-for-invisible-supply-chain-payloads
- https://securityboulevard.com/2026/03/an-evolving-glassworm-malware-is-making-the-rounds-of-code-repositories/
- https://www.aikido.dev/blog/glassworm-chrome-extension-rat
- https://www.scientificamerican.com/article/glassworm-malware-hides-in-invisible-open-source-code/

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

CAMPAÑA MASIVA DE DEVICE CODE PHISHING (OAUTH) CONTRA ORGANIZACIONES DE MICROSOFT 365

Investigadores de seguridad han alertado sobre una campaña activa de "Device Code Phishing" que ha impactado a más de 340 organizaciones globales. Esta operación utiliza la plataforma de Phishing-as-a-Service (PhaaS) EvilTokens para abusar del flujo de autorización de dispositivos de OAuth. La técnica es especialmente insidiosa porque permite obtener tokens de acceso persistentes que evaden el MFA y permanecen válidos incluso después de un restablecimiento de contraseña.

Resumen técnico:

- Técnica de ataque: Explotación del flujo de autorización de dispositivos de OAuth. El atacante genera un código mediante la API oficial de Microsoft y engaña al usuario para que lo autorice en microsoft.com/devicelogin.
- Infraestructura C2: Uso intensivo de la plataforma PaaS Railway.com. Se han identificado IPs específicas como 162.220.234.41, 162.220.234.66, 162.220.232.57, 162.220.232.99 y 162.220.232.235 que concentran el 84% de los eventos.
- Evasión de filtros: Uso de redireccionadores legítimos de Cisco, Trend Micro y Mimecast, combinados con Cloudflare Workers y Vercel, para ocultar las páginas de aterrizaje maliciosas de los sistemas de seguridad de correo.
- PhaaS (EvilTokens): Plataforma detectada en Telegram que ofrece soporte 24/7 y herramientas automatizadas para la generación de enlaces de redirección y bypass de filtros antispam.
- Grupos vinculados: Actividad atribuida a grupos de origen ruso como Storm-2372 y APT29.

Impacto potencial:

- Bypass efectivo de MFA: Al ser el propio usuario quien completa el flujo de autenticación (incluyendo el segundo factor), los sistemas de identidad generan tokens válidos directamente para el atacante.
- Persistencia extrema: Los tokens de acceso y actualización (refresh tokens) no se invalidan con el cambio de contraseña, permitiendo el acceso prolongado a la cuenta comprometida.
- Compromiso total de la suite M365: El atacante obtiene control total sobre correos electrónicos, calendarios, archivos en OneDrive/SharePoint y herramientas de colaboración como Teams.
- Vector para ataques BEC y movimiento lateral: La posesión de una identidad corporativa confiable facilita el fraude financiero (Business Email Compromise) y ataques dirigidos hacia otros empleados o socios de negocio.

Recomendaciones para mitigar el riesgo:

1. Revocación inmediata de tokens: Ante sospecha de compromiso, es mandatorio revocar todos los tokens de actualización desde el portal de Microsoft Entra ID o vía PowerShell (Revoke-MgUserSignInSession).
2. Bloqueo de infraestructura de Railway: Implementar reglas de bloqueo perimetral para las IPs de Railway identificadas y monitorear logs de inicio de sesión en busca de conexiones desde este proveedor de nube.
3. Restricción del flujo de dispositivos: Configurar políticas de Acceso Condicional para limitar o deshabilitar el flujo de "Device Code" en dispositivos que no sean corporativos o gestionados.
4. Monitoreo avanzado de logs de Sign-in: Crear alertas específicas para intentos de autenticación que utilicen el método "Device Code" y que provengan de ubicaciones o rangos de red inusuales.

Prioridad: Importante.

Ampliar Información:

- https://thehackernews.com/2026/03/device-code-phishing-hits-340-microsoft.html
- https://www.seguridadweb.net/blog/ciberseguridad/phishing-device-code-microsoft-365-empresas
- https://abnormal.ai/threat-intelligence/digest/device-code-phishing-campaign-hijacks-microsoft-365-accounts