GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1626

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

CVE-2026-40372 – ASP.NET CORE (ESCALADA DE PRIVILEGIOS)

Microsoft ha emitido una actualización de emergencia fuera de banda para corregir un fallo crítico en el framework ASP.NET Core. La vulnerabilidad permite a un atacante no autenticado falsificar tokens de seguridad y elevar sus privilegios hasta el nivel SYSTEM en entornos específicos.

Resumen técnico:

- Identificador principal: CVE-2026-40372.
- Severidad: 9.1 (Crítica) según la escala CVSS v3.1.
- Causa raíz: Una regresión en el paquete NuGet Microsoft.AspNetCore.DataProtection introdujo un error en la validación de firmas criptográficas.
- Mecanismo de falla: El cifrador autenticado calcula incorrectamente la etiqueta HMAC sobre bytes erróneos de la carga útil o, en ciertos casos, descarta el hash validado. Esto permite ataques de tipo "padding oracle" para falsificar cookies de autenticación y tokens antifalsificación.
- Estado de explotación: Divulgado el 21 de abril de 2026; se considera de alto riesgo para infraestructuras que no apliquen la rotación de llaves tras el parcheo.
- Versiones afectadas: Paquetes Microsoft.AspNetCore.DataProtection versiones 10.0.0 a 10.0.6 ejecutándose principalmente en Linux y macOS (o sistemas no-Windows).

Impacto potencial:

- Escalamiento total a SYSTEM: Un atacante puede obtener control absoluto sobre el host subyacente que ejecuta la aplicación web afectada.
- Secuestro de sesiones (Session Hijacking): Capacidad de falsificar cookies de identidad para suplantar a cualquier usuario, incluyendo administradores, sin conocer sus credenciales.
- Persistencia mediante tokens legítimos: Si un atacante generó tokens (API keys, enlaces de reseteo) durante la ventana de exposición, estos seguirán siendo válidos incluso después de actualizar el software.

Exposición y modificación de datos: Acceso no autorizado a archivos protegidos y capacidad para alterar información sensible procesada por la aplicación.

Recomendaciones de mitigación:

1. Actualización inmediata a la versión 10.0.7: Migrar de forma urgente todos los paquetes de DataProtection y revisar dependencias transitivas (ej. StackExchangeRedis).
2. Rotación obligatoria del "Key Ring": Es imperativo rotar las llaves de protección de datos para invalidar cualquier token o cookie maliciosa generada previamente por un atacante.
3. Auditoría de artefactos de larga duración: Revisar logs en busca de la creación inusual de llaves de API, sesiones persistentes o cambios de contraseña sospechosos durante el periodo vulnerable.
4. Implementación de estrategias SBOM: Utilizar herramientas de Software Bill of Materials para identificar rápidamente qué microservicios o contenedores están consumiendo la versión vulnerable de la librería.

Prioridad: Crítica.

Ampliar información:

- https://www.esecurityplanet.com/threats/cve-2026-40372-microsoft-patches-asp-net-core-privilege-escalation-vulnerability/
- https://arstechnica.com/security/2026/04/microsoft-issues-emergency-update-for-macos-and-linux-asp-net-threat/
- https://underc0de.org/foro/noticias-informaticas-120/cve-2026-40372-fallo-critico-en-asp-net-core/
- https://duendesoftware.com/blog/20260422-update-guidance-for-cve-2026-40372-aspnet-data-protection
- https://thehackernews.com/2026/04/microsoft-patches-critical-aspnet-core.html

CVE-2026-5752 – COHERE TERRARIUM SANDBOX (ESCAPE DE SANDBOX Y RCE)

Se ha detectado una vulnerabilidad crítica en Terrarium, una plataforma de ejecución de código basada en Python desarrollada por Cohere AI. El fallo permite a un atacante romper el aislamiento del sandbox y ejecutar comandos arbitrarios con privilegios de root en el proceso host de Node.js.

Resumen técnico:

- Identificador principal: CVE-2026-5752.
- Severidad: 9.3 (Crítica) según la escala CVSS.
- Causa raíz: Una configuración insegura de objetos globales (jsglobals) en el componente service.ts del entorno Pyodide (WebAssembly).
- Mecanismo de falla: El uso de objetos literales estándar para simular el entorno (como el objeto document) permite realizar un recorrido de la cadena de prototipos (Prototype Chain Traversal). Esto facilita el acceso al constructor Function para obtener globalThis y, eventualmente, alcanzar funciones internas peligrosas como require() de Node.js.
- Estado de explotación: Divulgado el 21 de abril de 2026. No existe un parche oficial ya que el repositorio ha sido archivado y no cuenta con soporte activo.
- Versiones afectadas: Todas las implementaciones basadas en el repositorio cohere-ai/cohere-terrarium.

Impacto potencial:

- Ejecución de código como root: Control total sobre el proceso host de Node.js y ejecución de comandos del sistema con máximos privilegios dentro del contenedor.
- Exfiltración de secretos y datos: Acceso no autorizado a archivos sensibles del sistema (ej. /etc/passwd) y robo de variables de entorno que contienen tokens de API o credenciales de bases de datos.
- Movimiento lateral en la red: Capacidad de alcanzar otros servicios, APIs internas o bases de datos que se encuentran en la misma red del contenedor, evadiendo perímetros de seguridad.
- Riesgo de escape del contenedor: Dependiendo de las capabilities y la configuración del runtime de Docker, el atacante podría escalar su control hacia el sistema operativo anfitrión.

Recomendaciones de mitigación:

1. Deshabilitar la ejecución de código externo: De ser posible, suspender temporalmente las funciones que permitan a usuarios finales enviar o ejecutar scripts en el sandbox de Terrarium.
2. Aplicar el principio de mínimos privilegios: Reconfigurar el despliegue para asegurar que el proceso host de Node.js se ejecute con un usuario sin privilegios y no como root.
3. Implementar segmentación de red estricta: Restringir el tráfico de salida (egress) del contenedor para evitar conexiones hacia otros microservicios o infraestructura interna.
4. Envolver en capas de aislamiento adicionales: Migrar la ejecución a entornos más robustos, como máquinas virtuales dedicadas (micro-VMs) o dominios totalmente separados, para limitar el radio de explosión en caso de compromiso.

Prioridad: Crítica.

Ampliar información:

- https://kb.cert.org/vuls/id/414811
- https://underc0de.org/foro/noticias-informaticas-120/cve-2026-5752-fallo-critico-en-terrarium-sandbox/
- https://thehackernews.com/2026/04/cohere-ai-terrarium-sandbox-flaw.html
- https://unaaldia.hispasec.com/2026/04/un-fallo-critico-en-cohere-ai-terrarium-permite-saltarse-el-sandbox-y-ejecutar-codigo-como-root.html/amp

CVE-2026-5760 – SGLANG (EJECUCIÓN REMOTA DE CÓDIGO - RCE)

Se ha identificado una vulnerabilidad crítica de inyección de comandos en SGLang, un framework de alto rendimiento para el despliegue de modelos de lenguaje (LLMs). El fallo permite a un atacante lograr la ejecución remota de código (RCE) mediante la carga de modelos maliciosos en formato GGUF, comprometiendo totalmente el servidor de inferencia.

Resumen técnico:

- Identificador principal: CVE-2026-5760.
- Severidad: 9.8 (Crítica) según la escala CVSS v3.1.
- Causa raíz: Uso de un entorno de renderizado de plantillas Jinja2 sin sandboxing (jinja2.Environment()) en lugar de una versión segura e inmutable.
- Mecanismo de falla: La vulnerabilidad reside en el endpoint de reclasificación (/v1/rerank). Un atacante puede crear un archivo de modelo GGUF con un parámetro tokenizer.chat_template manipulado que contenga un payload de Inyección de Plantillas del Lado del Servidor (SSTI). Al procesar una solicitud en dicho endpoint, SGLang ejecuta el código Python arbitrario incrustado en el modelo.
- Estado de explotación: Divulgado el 20 de abril de 2026 con Prueba de Concepto (PoC) pública disponible; se cataloga como un riesgo de cadena de suministro de modelos de IA.
- Versiones afectadas: Todas las versiones de SGLang que utilicen el endpoint de rerank de OpenAI sin el parche de sandboxing en serving_rerank.py.

Impacto potencial:

- Compromiso total del servidor: El atacante obtiene la capacidad de ejecutar comandos de sistema con los privilegios del proceso SGLang, pudiendo escalar a privilegios de root según la configuración del host.
- Ataque a la cadena de suministro de IA: Actores de amenazas pueden distribuir modelos "envenenados" en repositorios públicos como Hugging Face, logrando acceso masivo a infraestructuras de inferencia de empresas que descarguen dichos modelos.
- Exfiltración de datos y modelos: Acceso no autorizado a otros modelos almacenados en el servidor, pesos de modelos propietarios y datos sensibles procesados durante las sesiones de inferencia.
- Movimiento lateral en redes corporativas: El servidor comprometido puede ser utilizado como pivote para atacar otros activos dentro de la red interna, aprovechando la confianza del sistema de IA.

Recomendaciones de mitigación:

1. Implementar Sandboxing en Jinja2: Actualizar el código fuente para reemplazar jinja2.Environment() por ImmutableSandboxedEnvironment, restringiendo el acceso a funciones peligrosas del sistema operativo.
2. Verificación estricta de fuentes de modelos: Prohibir la carga de archivos GGUF o modelos desde repositorios públicos no verificados; implementar firmas criptográficas y verificación de hashes para cada modelo en producción.
3. Deshabilitar endpoints no utilizados: Si la funcionalidad de reranking no es esencial para la operación, se recomienda deshabilitar o restringir el acceso al endpoint /v1/rerank mediante reglas de firewall o WAF.
4. Aislamiento mediante contenedores endurecidos: Ejecutar las instancias de SGLang en entornos de contenedores aislados (como gVisor o Kata Containers) con sistemas de archivos de solo lectura y sin acceso a la red externa innecesaria.

Prioridad: Crítica.

Ampliar información:

- https://letsdatascience.com/news/sglang-enables-remote-code-execution-via-malicious-gguf-mode-963bf60d
- https://cybersecuritynews.com/hackers-weaponize-gguf-models/
- https://ciberconcienciadigital.com/noticia/603
- https://grabify.org/es/blog/sglang-cve-2026-5760-cvss-9-8-enables-rce-via-malicious-gguf-model-files/
- https://thehackernews.com/2026/04/sglang-cve-2026-5760-cvss-98-enables.html

MALWARE

CANISTERSPRAWL – WORM AUTOPROPAGANTE EN NPM Y PYPI (SUPPLY CHAIN)

Se ha identificado una campaña masiva de cadena de suministro denominada CanisterSprawl. Se trata de un gusano sofisticado que no solo actúa como un infostealer de credenciales, sino que utiliza los tokens robados para infectar automáticamente otros paquetes legítimos mantenidos por la víctima, extendiéndose por los ecosistemas de npm y PyPI.

Resumen técnico:

- Identificador principal: CanisterSprawl (relacionado con tácticas de TeamPCP).
- Tipo de amenaza: Gusano de cadena de suministro (Supply Chain Worm).
- Causa raíz: Inyección de código malicioso en versiones legítimas de herramientas populares de desarrollo (ej. pgserve, automagik) mediante el compromiso de cuentas de mantenedores.
- Mecanismo de falla: El malware se activa automáticamente durante la instalación del paquete mediante un hook de postinstall. Una vez ejecutado, recolecta secretos del entorno local y utiliza tokens de publicación de npm/PyPI para subir versiones "envenenadas" de todos los proyectos a los que el desarrollador tiene acceso.
- Infraestructura de exfiltración: Utiliza "canisters" de Internet Computer Protocol (ICP) (infraestructura descentralizada en blockchain) para el comando y control (C2), lo que hace que la infraestructura sea prácticamente inmune a bajas (takedowns) tradicionales por parte de autoridades.

Impacto potencial:

- Compromiso total de la infraestructura organizacional: Robo masivo de credenciales de nube (AWS, Azure, GCP), llaves SSH, archivos .env, configuraciones de Kubernetes/Docker y secretos de Terraform/Vault.
- Propagación viral en la cadena de suministro: El gusano convierte cada entorno de desarrollo infectado en un nuevo vector de ataque, publicando automáticamente versiones maliciosas en los perfiles de npm y PyPI de la víctima.
- Infección cruzada de ecosistemas: Capacidad de saltar de JavaScript a Python mediante la creación de archivos .pth maliciosos que se ejecutan cada vez que se inicia el intérprete de Python en el sistema.
- Robo de activos financieros y personales: Exfiltración de datos de billeteras de criptomonedas (MetaMask, Phantom, Exodus) y contraseñas almacenadas en navegadores basados en Chromium.

Recomendaciones de mitigación:

1. Rotación inmediata de credenciales: Si se sospecha de infección por versiones vulnerables (ej. pgserve >1.1.10), se deben rotar inmediatamente todas las llaves de acceso a nube, tokens de GitHub/npm y llaves SSH.
2. Deshabilitar scripts de instalación de forma global: Ejecutar el comando npm config set ignore-scripts true para evitar que los paquetes ejecuten código arbitrario durante el proceso de instalación.
3. Control estricto de egreso de red (Egress Filtering): Configurar los entornos de CI/CD para que los runners solo puedan conectarse a dominios explícitamente autorizados, bloqueando el acceso a dominios de ICP o webhooks desconocidos.
4. Implementación de Tokens de publicación con alcance limitado: Utilizar tokens de npm/PyPI con permisos granulares (scoped) para un solo paquete y rotarlos automáticamente de manera frecuente para limitar el radio de explosión.

Prioridad: Urgente.

Ampliar información:

- https://www.cmadrid.net/noticia/aed227a559f01fb1/un-gusano-autopropagante-de-la-cadena-de-suministro-secuestra-paquetes-n
- https://www.stepsecurity.io/blog/pgserve-compromised-on-npm-malicious-versions-harvest-credentials
- https://www.infoworld.com/article/4162198/malicious-pgserve-automagik-developer-tools-found-in-npm-registry.html
- https://thehackernews.com/2026/04/self-propagating-supply-chain-worm.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

TRES ZERO-DAYS EN MICROSOFT DEFENDER EXPLOTADOS ACTIVAMENTE

Se ha confirmado la explotación en entornos reales de tres vulnerabilidades críticas en Microsoft Defender, denominadas BlueHammer, RedSun y UnDefend. Estos fallos, divulgados originalmente como zero-days por el investigador "Chaotic Eclipse", permiten desde la escalada de privilegios hasta la degradación total de las capacidades de protección del endpoint.

Resumen técnico:

- Los exploits fueron publicados en GitHub como medida de protesta ante la gestión de reportes de Microsoft. Huntress Labs y otros investigadores han confirmado su uso en ataques dirigidos (específicamente vinculados a actividad de tipo "hands-on-keyboard").
- BlueHammer (CVE-2026-33825): Una condición de carrera (TOCTOU) en el flujo de actualización de firmas que permite redirigir lecturas de archivos hacia el hive SAM, obteniendo hashes NTLM y privilegios SYSTEM.
- RedSun: Similar a BlueHammer, pero afecta al servicio TieringEngineService.exe. Sigue siendo funcional en sistemas totalmente parcheados (Windows 10/11 y Server 2019+) tras el Patch Tuesday de abril.
- UnDefend: Una técnica de degradación que bloquea las actualizaciones de definiciones de Defender, dejando al sistema "ciego" ante nuevas amenazas sin generar alertas de fallo crítico.
- Estado: Solo BlueHammer cuenta con parche oficial (CVE-2026-33825). RedSun y UnDefend permanecen sin corrección técnica definitiva a la fecha.

Impacto potencial:

- Compromiso total del sistema (Privilegios SYSTEM): El uso de BlueHammer o RedSun permite a un atacante con bajos privilegios ejecutar código con el máximo nivel de confianza del sistema operativo.
- Extracción de credenciales críticas: Acceso directo a la base de datos SAM y secretos de seguridad que permiten ataques de tipo Pass-the-Hash y movimiento lateral inmediato.
- Invisibilidad operativa: Mediante UnDefend, un atacante puede reducir progresivamente la fidelidad de detección del antivirus, permitiendo el despliegue de malware adicional sin ser detectado por el motor heurístico.
- Abuso de la "Confianza del Defensor": Las vulnerabilidades no explotan errores de memoria tradicionales, sino la lógica de cómo Defender interactúa con el sistema de archivos, convirtiendo la herramienta de seguridad en el propio vector de entrada.

Recomendaciones para mitigar el riesgo:

1. Aplicar parches de abril de 2026 inmediatamente: Instalar las actualizaciones de seguridad para mitigar el vector de BlueHammer (CVE-2026-33825) en todos los activos Windows.
2. Monitoreo de comportamientos anómalos: Vigilar la ejecución de comandos de enumeración sospechosos (whoami /priv, cmdkey /list) y el staging de archivos en directorios de poco ruido como "Pictures" o subcarpetas de "Downloads".
3. Implementar Defensa en Profundidad (NDR): No depender exclusivamente del EDR/Antivirus; utilizar visibilidad a nivel de red para detectar anomalías de tráfico y escaladas de privilegios que el agente local podría no reportar si ha sido degradado.

4. Auditoría de procesos hijos de Explorer: Investigar cualquier instancia de cmd.exe o ejecutables desconocidos (ej. z.exe, FunnyApp.exe) que se originen bajo el proceso de Explorer o que intenten manipular el registro de actualizaciones de Defender.

Prioridad: Importante.

Ampliar Información:

- https://www.antifraude.co/tres-vulnerabilidades-zero-day-en-microsoft-defender-ponen-en-riesgo-millones-de-usuarios/
- https://thehackernews.com/2026/04/three-microsoft-defender-zero-days.html
- https://www.helpnetsecurity.com/2026/04/17/microsoft-defender-zero-days-exploited/
- https://www.vectra.ai/blog/when-the-defender-becomes-the-door-bluehammer-redsun-and-undefend-in-the-wild