

GammaCS-CERT
By Gamma Ingenieros



Boletín de Ciberseguridad Semanal

Edición °3826



BOLETÍN DE CIBERSEGURIDAD SEMANTAL

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 para nuestros 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	1	0

VULNERABILIDADES

SOLARWINDS ACCESS RIGHTS MANAGER (ARM) – VULNERABILIDAD CRÍTICA DE CLAVE ESTÁTICA HARDCODED PERMITE EJECUCIÓN REMOTA DE CÓDIGO NO AUTENTICADA (CVE-2026-28326)

SolarWinds ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica de ejecución remota de código (RCE) sin autenticación en Access Rights Manager (ARM). La falla se debe a la presencia de una clave secreta estática e idéntica en todas las instalaciones del producto, la cual permite a un atacante no autenticado evadir el control de acceso en el servicio gRPC (puerto TCP 55555) y alcanzar un punto de deserialización no segura mediante .NET Remoting y BinaryFormatter, logrando la ejecución de código con máximos privilegios (NT AUTHORITY\SYSTEM).

Resumen técnico:

- Identificador principal: CVE-2026-28326.
- Severidad: Crítica (CVSS v3.1: 8.8 en postura adyacente AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H; escala a 9.8 AV:N en entornos de red plana no segmentados).
- Causa raíz: Uso de clave secreta estática hardcoded en el instalador (CWE-798 / CWE-321), falta de validación de contexto local en mecanismos de autenticación alternativos y deserialización no segura de datos mediante BinaryFormatter en .NET Remoting (CWE-502).
- Mecanismo de falla:
- El servicio gRPC que escucha en el puerto TCP 55555 solicita certificados de cliente TLS pero no exige su presentación de forma obligatoria, permitiendo a un atacante completar el saludo TLS de manera anónima.
- Un canal de autenticación de respaldo en la aplicación permite a las conexiones sin certificado autenticarse mediante un token HMAC en los encabezados HTTP/2, calculado a partir de una clave secreta estática incluida de fábrica en el instalador del software.
- Dado que la clave es idéntica en todas las instalaciones y los campos firmados son controlados por el cliente, un atacante remoto puede generar tokens válidos sin interacción con el servidor ni desafíos de autenticación.
- Una vez superado el control de acceso, la conexión accede a un flujo dúplex de mensajes .NET Remoting que son deserializados con BinaryFormatter bajo una lista de bloqueo de tipos insuficiente, permitiendo ejecutar comandos en el sistema operativo subyacente con privilegios de NT AUTHORITY\SYSTEM.
- Estado de explotación: Divulgada oficialmente por SolarWinds el 17 de septiembre de 2026 (corregida en ARM 2026.2.1.7). Se cuenta con análisis técnico detallado e investigación pública con herramientas de detección segura de parcheo. No se registra evidencia de explotación activa en el entorno real previa a la divulgación.
- Versiones afectadas: SolarWinds Access Rights Manager (ARM) en versiones 2026.2.0.42 y anteriores (incluyendo la rama 2026.2 y versiones que alcanzaron el Fin de Soporte/EoL como la serie 2023.2.x).

Impacto potencial:

- Ejecución remota de código con máximos privilegios (NT AUTHORITY\SYSTEM): Permite a un atacante no autenticado tomar control absoluto del sistema operativo del servidor que aloja la solución ARM.
- Compromiso de la infraestructura de gestión de identidades y accesos: Al ser una herramienta de gobernanza de derechos de acceso, la toma de control permite manipular permisos en Active Directory, servidores de archivos, Microsoft Exchange y SharePoint.
- Movimiento lateral y escalada de privilegios en el dominio: Facilita la extracción de credenciales administrativas y la reutilización de los permisos delegados de ARM para extender el ataque hacia otros activos críticos de la organización.
- Movimiento lateral y despliegue de ransomware corporativo: Sirve como punto de apoyo perimetral para establecer túneles SOCKS/SSH reversos hacia la red interna, permitiendo el despliegue posterior de ransomware en endpoints de la organización.
- Despliegue de malware y persistencia sigilosa: Habilita la instalación de ejecutable maliciosos, puertas traseras y la creación de tareas programadas evasivas en el servidor comprometido.

Recomendaciones de mitigación:

1. Aplicación prioritaria del parche de seguridad: Actualizar inmediatamente SolarWinds Access Rights Manager a la versión 2026.2.1.7 o superior, la cual elimina por completo el canal de autenticación inseguro basado en clave estática.
2. Restricción perimetral e interna del puerto TCP 55555: Configurar reglas estrictas en firewalls de red y de host para limitar el acceso al puerto TCP 55555 exclusivamente a las direcciones IP de los componentes y recolectores autorizados de ARM.
3. Auditoría e inspección de indicadores de compromiso (IoCs) previa a la actualización: Revisar la lista de conexiones activas en memoria (GET /api/armconfig/network/Connections) buscando registros con IsAuthenticated: false y ClientCertThumbPrint poblado antes de reiniciar el servicio para aplicar el parche.
4. Planes de actualización para versiones EoL y aislamiento temporal: En entornos que ejecuten versiones discontinuadas (como ARM 2023.2.x), realizar la migración obligatoria utilizando al menos la versión 2023.2.4 como base para alcanzar la versión corregida.

Prioridad: Crítica.

Ampliar información:

- <https://www.heise.de/en/news/Unauthorized-access-to-SolarWinds-Access-Rights-Manager-possible-11460067.html>
- <https://www.verisq.ai/intelligence/solarwinds-patches-arm-hard-coded-key-flaw-enabling-unauthenticated-rce-66250>
- <https://www.securityweek.com/solarwinds-patches-critical-rce-flaws-in-observability-self-hosted/>
- <https://thehackernews.com/2026/09/solarwinds-patches-arm-hard-coded-key.html>
- <https://bishopfox.com/blog/detecting-solarwinds-arm-cve-2026-28326>

NEXT.JS (VERCEL) – VULNERABILIDAD CRÍTICA EN IMAGERESPONSE Y LIBRERÍA SATORI PERMITE EJECUCIÓN REMOTA DE CÓDIGO MEDIANTE INYECCIÓN DE SVG MANIPULADO (CVE-2026-94545)

Vercel ha publicado una actualización de seguridad urgente para corregir una vulnerabilidad crítica (CVE-2026-94545) en la función ImageResponse de Next.js (next/og). El fallo, originado en la biblioteca subyacente Satori, se debe a la falta de sanitización al escapar valores controlados por los usuarios antes de insertarlos en el marcado SVG generado. Al ejecutarse en el entorno de ejecución Node.js, esta inyección permite romper el contexto del SVG y concatenar fallos en dependencias del sistema, lo que habilita la ejecución remota de código (RCE) en el servidor sin requerir autenticación previa.

Resumen técnico:

- Identificador principal: CVE-2026-94545 (GHSA-vcvr-r3jv-pc5j en Next.js / GHSA-wx4j-mvgx-mqwp en Satori).
- Severidad: Crítica (CVSS v4.0: 9.5 / CVSS v3.1: 9.5).
- Causa raíz: Escapado y codificación insuficiente de salida (CWE-116) en la librería Satori (versiones 0.0.27 a 0.33.4) al convertir marcado HTML/CSS a SVG dentro del proceso de generación de imágenes Open Graph y vistas previas sociales.
- Mecanismo de falla:
- La aplicación toma parámetros de la solicitud HTTP o datos controlados por el usuario (como texto leído desde la URL, variables de ruta o campos de entrada) y los incluye en los componentes de ImageResponse.
- La biblioteca Satori no escapa adecuadamente estos valores al serializarlos dentro del contenido, atributos o estilos CSS del documento SVG resultante.
- La carga manipulada es interpretada por el renderizador como marcado SVG/XML ejecutable en lugar de texto plano, logrando romper el contenedor e inyectar entidades XML o elementos no autorizados.

- Al procesarse en el entorno de ejecución Node.js (runtime predeterminado en Next.js), los datos manipulados alcanzan vulnerabilidades en librerías nativas subyacentes del paquete, derivando en la ejecución arbitraria de comandos en el servidor.
- Estado de explotación: Divulgada y corregida por Vercel el 22 de septiembre de 2026. Se registran pruebas de concepto (PoC) públicas e investigaciones técnicas detalladas; no se ha confirmado explotación maliciosa activa previa en el entorno real al momento de la publicación.
- Versiones afectadas: Next.js versiones 16.2.0 hasta 16.3.5 cuando utilizan el entorno Node.js (la rama 15.x no resulta vulnerable a este vector de RCE, aunque la versión 15.5.26 añade refuerzos de seguridad). La librería Satori en versiones 0.0.27 a 0.33.4.

Impacto potencial:

- Ejecución remota de código (RCE) en el servidor: Permite a un atacante no autenticado ejecutar comandos del sistema operativo en el contexto de seguridad del proceso Node.js que ejecuta la aplicación web.
- Compromiso y exfiltración de información confidencial: Otorga capacidad para acceder a variables de entorno del servidor, claves de API, credenciales de bases de datos, tokens de sesión y archivos del sistema.
- Interrupción del servicio y sobrecostos operativos: La explotación de solicitudes maliciosas puede provocar el colapso recurrente de las funciones serverless o trabajadores de Node.js, generando denegación de servicio o incrementos anómalos en los costos de infraestructura en la nube.
- Vector de ataque para movimiento lateral: El compromiso del servidor de aplicaciones web puede ser utilizado por el atacante como punto de apoyo perimetral para pivotar hacia redes internas, microservicios adyacentes o bases de datos corporativas.

Recomendaciones de mitigación:

1. Actualización inmediata a la versión corregida: Desplegar de forma prioritaria la actualización a Next.js versión 16.3.6 (o actualizar la librería Satori a la versión 0.33.5 en proyectos independientes) para aplicar el parche en la lógica de escapado de SVG.
2. Saneamiento y restricción de entradas de usuario en imágenes: En caso de no poder actualizar inmediatamente, evitar la inclusión de valores o datos no confiables provistos por los usuarios dentro de los atributos, contenido o estilos renderizados por ImageResponse.
3. Evaluación de migración hacia Edge Runtime: Considerar la configuración de las rutas de generación de imágenes en el entorno Edge Runtime (Edge ImageResponse), el cual no se ve afectado por la vía de ejecución remota de código de Node.js.
4. Verificación directa de versiones y depuración de despliegues: Comprobar la versión instalada directamente en el paquete de Next.js (ya que Satori se empaqueta de forma interna) y proceder a eliminar o reconstruir vistas previas de despliegue (deploy previews) expuestas públicamente.

Prioridad: Crítica.

Ampliar información:

- <https://blog.elhacker.net/2026/09/grave-vulnerabilidad-en-imageresponse.html>
- <https://www.netlify.com/changelog/2026-09-22-nextjs-imageresponse-vulnerability/>
- <https://mallory.ai/vulnerabilities/CVE-2026-94545>
- <https://nextjs.org/blog/nextjs-security-update-september-22-2026>
- <https://aviatrix.ai/threat-research-center/nextjs-imageresponse-cve-2026-94545-server-code-execution/>

WORDPRESS CORE – VULNERABILIDAD CRÍTICA DE PATH TRAVERSAL EN LA RESOLUCIÓN DE PLANTILLAS PERMITE INCLUSIÓN DE ARCHIVOS LOCALES (LFI) Y EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-87902)

El equipo de seguridad de WordPress ha lanzado actualizaciones de emergencia para corregir una vulnerabilidad crítica de path traversal e inclusión de archivos locales (LFI) sin autenticación en el núcleo de WordPress Core. La falla, localizada en la lógica de resolución de plantillas de páginas (`get_page_template()` / `locate_template()`), permite a un atacante remoto no autenticado forzar al sistema a incluir archivos .php locales fuera del directorio del tema activo. En entornos con configuraciones específicas (como la presencia de `pearcmd.php` y la directiva `register_argc_argv` activada), el fallo escala a ejecución remota de código (RCE) y compromiso total del servidor web.

Resumen técnico:

- Identificador principal: CVE-2026-87902 (GHSA-7hp8-65ch-5whp).
- Severidad: Crítica (CVSS v4.0: 9.2 / CVSS v3.1: 8.1 - 9.2).
- Causa raíz: Inclusión de archivos locales / Traversal de directorio (CWE-98 / CWE-22) en la función `locate_template()` (`wp-includes/template.php`) debido a una decodificación doble insegura con `urldecode()` sobre la variable de consulta `pagename` sin validación previa mediante `validate_file()`.
- Mecanismo de falla:
- El atacante envía una solicitud (habitualmente POST) manipulada hacia el sitio web, incluyendo un `page_id` válido y una secuencia de salto de directorio (path traversal) doblemente codificada dentro de la variable `pagename`.
- La función `get_page_template()` aplica `urldecode()` sobre `pagename`, convirtiendo la cadena codificada (como `%252e%252e%252f`) en secuencias de recorrido de ruta (`../`) para construir un candidato de plantilla con la estructura `page-{decoded}.php`.

- La función `locate_template()` concatena esta ruta al directorio del tema activo y comprueba la existencia del archivo sin validar si la ruta resultante permanece dentro de los límites permitidos del tema.
- Al cumplirse las condiciones del tema (por ejemplo, temas con carpetas superiores iniciadas con `page-`, como Twenty Twelve, Twenty Fourteen, Neve, Hestia o Sydney), `load_template()` incluye el archivo `.php` local. Si el servidor cuenta con bibliotecas como `pearcmd.php` de PEAR, el atacante puede escribir y ejecutar código PHP malicioso en un directorio temporal (`/tmp`), logrando RCE.
- Estado de explotación: Divulgada y corregida el 22 de septiembre de 2026. Se cuenta con pruebas de concepto (PoC) públicas y reportes de escaneos masivos e intentos de explotación activa en el entorno real a pocas horas de la publicación del parche.
- Versiones afectadas: WordPress Core en todas sus versiones desde la 4.7.0 hasta la 7.1.1 (corregido en la versión 7.1.2 y en los backports de seguridad 7.0.6, 6.9.9, 6.8.10, 6.7.9, 6.6.9 hasta la rama 4.7.37).

Impacto potencial:

- Inclusión no autorizada de archivos PHP locales (LFI): Permite a atacantes no autenticados ejecutar cualquier archivo `.php` legible presente en el sistema de archivos del servidor web fuera del directorio del tema.
- Ejecución remota de código (RCE) en el servidor: Bajo configuraciones vulnerables del servidor (como imágenes Docker oficiales de PHP o entornos cPanel con `register_argc_argv=On`), habilita la ejecución de comandos arbitrarios con los privilegios del servicio web.
- Compromiso total de la instalación de WordPress: Otorga la capacidad de desplegar web shells, modificar archivos del núcleo o de plugins y tomar control administrativo del sitio web.
- Exfiltración de credenciales y datos confidenciales: Facilita la lectura de archivos de configuración con claves de bases de datos, datos de usuarios y secretos de la aplicación.

Recomendaciones de mitigación:

1. Actualización prioritaria de WordPress Core: Actualizar de inmediato a WordPress versión 7.1.2 o aplicar el parche de seguridad correspondiente a la rama en uso (7.0.6, 6.9.9, 6.8.10, 6.7.9, etc.).
2. Endurecimiento de la configuración de PHP: Desactivar la directiva `register_argc_argv` (`register_argc_argv = Off`) en el archivo `php.ini` y eliminar o restringir el acceso a scripts de utilidades no esenciales como `pearcmd.php`.
3. Despliegue de reglas en WAF (Virtual Patching): Activar reglas de inspección en el Firewall de Aplicaciones Web (WAF) para bloquear peticiones con secuencias de traversal codificadas en el parámetro `pagename`.
4. Auditoría de logs e inspección de archivos temporales: Auditar los registros de acceso HTTP en busca de solicitudes POST inusuales dirigidas al front-end con comandos PEAR y revisar directorios escribibles (como `/tmp` o `wp-content`) en busca de archivos `.php` sospechosos.

Prioridad: Crítica.

Ampliar información:

- <https://www.ionix.io/threat-center/cve-2026-87902/>
- <https://www.wordfence.com/blog/2026/09/psa-critical-unauthenticated-path-traversal-vulnerability-patched-in-wordpress-core/>
- <https://www.kaspersky.com/blog/cve-2026-87902-wordpress-vulnerability/56459/>
- <https://equixly.com/blog/2026/09/24/cve-2026-87902-from-wordpress-path-traversal-to-rce-via-pear/>
- <https://cloudlinux.zendesk.com/hc/en-us/articles/30509944684188-CVE-2026-87902-WordPress-Core-Path-Traversal-in-Template-Resolution>

MALWARE

MALWARE — CHAINSCRIPT: NUEVO TROYANO DE ACCESO REMOTO BASADO EN NODE.JS UTILIZA LA BLOCKCHAIN DE POLYGON PARA ROTAR SU INFRAESTRUCTURA DE COMANDO Y CONTROL (C2)

Investigadores de ciberseguridad del Adversary Pursuit Group de Blackpoint Cyber han documentado la aparición de ChainScript, un troyano de acceso remoto (RAT) no detectado previamente y desarrollado sobre el entorno Node.js. El malware se distribuye mediante engaños de ingeniería social de tipo ClickFix e instaladores MSI falsos disfrazados de aplicaciones populares como Spotify, Zoom Workplace y Microsoft Teams. Su característica técnica más destacada es el uso de un contrato inteligente en la red blockchain de Polygon como resolutores descentralizados para descubrir de forma dinámica la dirección activa de su servidor de Comando y Control (C2) mediante WebSockets, complicando las labores de inactivación y bloqueo de su infraestructura.

Resumen técnico:

- Identificador principal: Troyano de Acceso Remoto (RAT) ChainScript (asociado a nombres de compilación como ComponentTask33, UpdateDigital, HostShared y OrchidViolet66).
- Tipo de amenaza: Troyano de Acceso Remoto (Remote Access Trojan - RAT) / Malware basado en Blockchain (técnica EtherHiding) / Infostealer.
- Mecanismo de acceso e infección: La cadena de infección inicia mediante la técnica ClickFix, donde sitios web maliciosos engañan a la víctima para ejecutar comandos manipulados a través de la ventana Ejecutar (Win+R) o consolas del sistema. Esto desencadena la descarga de un instalador MSI (msiexec.exe) que ejecuta scripts ocultos en PowerShell y VBScript. Estos componentes despliegan un ejecutable legítimo de Node.js y el agente malicioso escrito en JavaScript dentro de directorios del perfil de usuario (%LOCALAPPDATA%) con nombres que simulan ser componentes oficiales de Microsoft, logrando ejecutarse sin requerir privilegios de administrador.
- Resolución de C2 mediante Smart Contracts y capacidades del agente:
- Descubrimiento C2 vía Polygon (EtherHiding): El agente consulta un contrato inteligente en la red Polygon (chain ID 137) enviando peticiones eth_call. El contrato responde con la dirección WebSockets (ws:// o wss://) del servidor activo. Esto permite a los operadores rotar los servidores de mando de forma remota modificando el contrato en la cadena de bloques, evitando la invalidez de la muestra en disco por bloqueo de IPs o dominios.
- Capacidades operativas: Proporciona control remoto interactivo mediante consolas CMD y PowerShell, gestión del sistema de archivos (lectura, escritura y borrado), captura de pantallas del escritorio, ejecución arbitraria de código JavaScript, capacidad de autodesinstalación/actualización e inventariado de billeteras de criptomonedas (extensiones de navegador y aplicaciones de escritorio).
- Estado de actividad: Campaña activa reportada a mediados de septiembre de 2026, dirigida a usuarios de sistemas operativos Windows mediante la suplantación de software corporativo y de entretenimiento

Impacto potencial:

- Toma de control total y ejecución remota de comandos: Otorga al atacante un shell interactivo completo (CMD/PowerShell) para ejecutar comandos arbitrarios, explorar el sistema de archivos y manipular procesos con el nivel de privilegios del usuario infectado.
- Compromiso y exfiltración de billeteras de criptomonedas: Escanea e inventaría activamente las billeteras digitales instaladas en el sistema y en las extensiones del navegador, exponiendo los activos criptográficos de la víctima a robos o exfiltración secundaria.
- Despliegue de payloads secundarios y escalada del ataque: Funciona como un cargador (dropper) capaz de descargar y ejecutar código malicioso adicional en la máquina comprometida, tal como ransomware, infostealers o herramientas de acceso persistente.
- Evasión de defensas y alta resiliencia de la infraestructura C2: Al utilizar la blockchain de Polygon como resolutor externo, el canal de comando del malware resiste las solicitudes de baja (takedown) tradicionales y las listas negras estáticas de dominios e IPs.

Recomendaciones de mitigación:

1. Monitoreo e inspección de ejecuciones de Node.js y scripts: Configurar reglas en soluciones EDR para detectar la ejecución anómala de binarios node.exe o scripts VBS/PowerShell lanzados desde rutas de perfil de usuario (AppData\Local\...) derivados de msixexec.exe o wscript.exe.
2. Supervisión de tráfico RPC a Blockchain y WebSockets: Auditar y alertar sobre conexiones salientes de aplicaciones no habituales hacia nodos de la red Polygon o Ethereum seguidas del establecimiento inmediato de sesiones WebSockets (ws:// / wss://).
3. Capacitación del personal contra técnicas de ingeniería social ClickFix: Educar a los colaboradores sobre los riesgos de copiar y pegar comandos en la consola de comandos o en la ventana Ejecutar de Windows derivados de mensajes emergentes o solicitudes en sitios web.
4. Auditoría de tareas programadas y mecanismos de persistencia local: Monitorear la creación de tareas programadas o modificaciones en la clave del Registro HKCU\Software\Microsoft\Windows\CurrentVersion\Run iniciadas por cuentas de usuario estándar.

Prioridad: Urgente.

Ampliar información:

- <https://thehackernews.com/2026/09/clickfix-lures-deploy-chainscript-rat.html>
- <https://www.pcrisk.com/removal-guides/35965-chainscript-rat>
- <https://csirtasobancaria.com/chainscript-nuevo-rat-basado-en-node-js-con-capacidades-de-acceso-remoto>
- <https://hamerintel.com/data/articles/18460>
- <https://www.moncloa.com/2026/09/22/chainscript-malware-blockchain-polygon-c2-3435360/>

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

ORKES CONDUCTOR – EXPLOTACIÓN ACTIVA DE VULNERABILIDAD CRÍTICA PRE-AUTENTICACIÓN PERMITE EJECUCIÓN REMOTA DE CÓDIGO EN PLATAFORMAS DE ORQUESTACIÓN EMPRESARIAL (CVE-2026-58138)

Fortinet y diversos centros de inteligencia de amenazas (incluyendo FortiGuard Labs y HoneyNet UNAMex) han emitido alertas de brote urgente tras confirmar la explotación activa en el entorno real de una vulnerabilidad crítica de ejecución remota de código (RCE) pre-autenticación que afecta a Orkes Conductor. La falla permite a atacantes remotos enviar definiciones de flujos de trabajo manipuladas con expresiones maliciosas en JavaScript o Python a la API de la plataforma. Al procesarse en evaluadores GraalVM sin aislamiento adecuado (sandbox), el atacante puede escapar del entorno de ejecución y ejecutar comandos arbitrarios en el sistema operativo con los privilegios del servidor.

Resumen técnico:

- Identificador principal: CVE-2026-58138 (CWE-94 - Inyección de Código / Control Inadecuado de Generación de Código).
- Severidad: Crítica / Alta Importancia (CVSS v3.1: 9.8 / CVSS v4.0: 9.3 - Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H).
- Causa raíz: Configuración insegura y falta de aislamiento en los evaluadores de scripts de GraalVM (permisos de acceso al host sin restricciones como HostAccess.ALL o allowAllAccess(true)).
- Mecanismo de falla:
- El atacante envía una solicitud HTTP POST no autenticada hacia el endpoint de la API de flujos de trabajo de Orkes Conductor.
- La carga útil contiene una definición de flujo de trabajo en línea con expresiones maliciosas escritas en JavaScript o Python asociadas a tipos de tareas INLINE, LAMBDA, DO_WHILE y SWITCH.
- El motor GraalVM procesa las expresiones sin las restricciones de un entorno aislado (sandbox), permitiendo al script interactuar con clases internas mediante reflexión de Java (Java reflection) o invocaciones directas a subprocesos (Runtime.getRuntime().exec() / ProcessBuilder).
- Esto permite romper los límites de la aplicación y ejecutar comandos arbitrarios del sistema operativo con el nivel de privilegios del proceso del servidor Conductor.
- Estado de actividad: Confirmada la explotación activa a nivel global a mediados de septiembre de 2026. Telemetría de seguridad registra miles de intentos de ataque automatizados y escaneos oportunistas originados desde múltiples regiones.
- Versiones afectadas: Orkes Conductor en todas sus versiones desde la 3.21.21 hasta anteriores a la 3.30.2.

Impacto potencial:

- Ejecución remota de código con privilegios del servicio: Permite a un atacante no autenticado tomar control del servidor de aplicaciones web y ejecutar comandos arbitrarios en el sistema operativo anfitrión.
- Compromiso estructural de la infraestructura de microservicios: Al tratarse de un motor de orquestación, el compromiso del servidor otorga acceso a las bases de datos, APIs e integraciones de negocio coordinadas por los flujos de trabajo.
- Exfiltración de credenciales y secretos de integración: Permite extraer claves de API, tokens de sesión, certificados y secretos de configuración almacenados o procesados en las tareas de la plataforma.
- Vector de ataque para movimiento lateral y despliegue de malware: Otorga un punto de apoyo perimetral para pivotar hacia redes internas, entornos en la nube o ejecutar cargas maliciosas secundarias en la infraestructura corporativa.

Recomendaciones para mitigar el riesgo:

1. Actualización prioritaria a la versión 3.30.2 o superior: Desplegar inmediatamente el parche oficial liberado por el fabricante para corregir la configuración insegura de los evaluadores GraalVM.
2. Restricción y aislamiento perimetral de la API: Bloquear la exposición pública no autorizada de los endpoints de la API de flujos de trabajo, situándolos detrás de proxies inversos, WAFs o redes privadas con autenticación estricta.
3. Configuración de seguridad en evaluadores dinámicos: En implementaciones personalizadas, asegurar que los motores de scripting deshabiliten explícitamente el acceso total al host (`allowAllAccess(false)`).
4. Auditoría de logs y monitoreo de procesos: Inspeccionar registros HTTP en busca de peticiones POST inusuales hacia la API con funciones de reflexión o comandos de consola, y monitorear la creación de procesos hijos no autorizados generados por el servicio Conductor.

Prioridad: Urgente.

Ampliar Información:

- <https://blog.elhacker.net/2026/09/explotan-vulnerabilidad-critica-de-rce.html>
- <https://blog.enhacke.com/explotacion-critica-en-orkes-conductor-rce-sin-autenticacion/>
- <https://es.honeynet.org.mx/posts/critical-pre-auth-rce-in-orkes-conductor-workflow-platform-exploited-in-the-wild-es/>
- <https://ciberseguridadlatam.com/orkes-conductor-expone-ejecucion-remota-sin-autenticacion-explotacion-activa-confirmada/>
- <https://www.fortiguard.com/lat/outbreak-alert/orkes-conductor-rce>