Alerta

Técnica

Vulnerabilidad explotada en VMware

COLCERT AL-20251002-077

TLP:CLEAR

Se ha identificado la vulnerabilidad **CVE-2025-41244** en **VMware**, actualmente bajo explotación activa por actores vinculados a China, que permite la **elevación de privilegios** en entornos virtualizados críticos. Este escenario incrementa de manera significativa el riesgo de accesos persistentes y movimientos laterales en infraestructuras estratégicas.

Aunque el impacto inicial se concentra en ataques dirigidos, existe una alta probabilidad de expansión de campañas en el corto plazo, lo **que podría generar disrupciones en cadenas de suministro y servicios en la nube**. El nivel de incertidumbre se considera alto, dado que la explotación ha sido confirmada y podría escalar con rapidez en foros clandestinos. En este contexto, la toma de decisiones anticipada debe priorizar parches inmediatos, segmentación de entornos y monitoreo reforzado para mitigar el riesgo de comprometer la continuidad de negocio.

VMware Cloud Foundation™

VMware vSphere® Foundation

VMware Aria™

Vulnerabilidad identificada

CVE	PRODUCTOS AFECTADOS	SCORE CVSS	DESCRIPCIÓN
CVE-2025-41244	• VMware Cloud Foundation 4.x, 5.x, 9.x.x.x, 13.x.x.x (Windows, Linux). • VMware vSphere Foundation 9.x.x.x, 13.x.x.x (Windows, Linux). • VMware Aria Operations 8.x. • VMware Tools 11.x.x, 12.x.x, 13.x.x (Windows, Linux). • VMware Telco Cloud Platform 4.x, 5.x. • VMware Telco Cloud Infrastructure 2.x, 3.x	**7.8 (Alto)**	Vulnerabilidad de escalamiento de privilegios locales que permite a un ciberdelincuente sin privilegios ejecutar código con privilegios de *root* en una máquina virtual, aprovechando una función que interpreta patrones regex de forma amplia y permite la carga de binarios maliciosos en directorios de escritura como /tmp/. Explotada como Zero-Day desde octubre de 2024.

NIVEL DE RIESGO

ALTO

COLCERT

¿Cómo se podrían explotar esta debilidad?

La explotación observada de **CVE-2025-41244** sigue el siguiente patrón:

1. **Acceso inicial requisito**: la vulnerabilidad es de escalamiento local de privilegios, por lo que el ciberdelincuente ya debe disponer de algún nivel de acceso en la máquina virtual. Por ejemplo, una cuenta no privilegiada conseguida por phishing, explotación previa o credenciales débiles.

2. **Aprovechamiento de la lógica de "service discovery"**: un componente de VMware (por ejemplo, parte de VMware Tools / Aria Operations) ejecuta rutinas de detección o consulta de versiones que, internamente, usan patrones (regex) para identificar binarios que exponen servicios.

3. **Coincidencia con binarios en rutas escritas por usuarios**: debido a patrones demasiado permisivos, la lógica puede coincidir con binarios alojados en directorios con permiso de escritura para usuarios no privilegiados, por ejemplo /tmp, permitiendo que un binario no-sistema sea invocado por el proceso de mayor privilegio.

4. **Invocación en contexto privilegiado**: cuando la herramienta invoca el "comando de versión" del binario coincidente, lo ejecuta con el contexto del servicio (más privilegiado), lo que permite que el atacante ejecute código con esos privilegios y alcance *root* dentro de la VM.
   Posibles consecuencias posteriores: tras la elevación, el ciberdelincuente puede instalar persistencia, moverse lateralmente desde la VM afectada, capturar datos, o realizar acciones de sabotaje.

Impacto para Colombia y la región

- **Sectores afectados**: salud, financiero, gobierno, electricidad, TIC, transporte, educación, comercio, industria y turismo.

- **Riesgo alto**: la vulnerabilidad permite escalamiento local de privilegios en máquinas virtuales ampliamente desplegadas en infraestructuras críticas. En la región, la elevada adopción de entornos virtualizados por proveedores de servicios, entidades gubernamentales y el sector salud, junto con prácticas heterogéneas de parcheo y segmentación, incrementa significativamente la probabilidad de compromisos exitosos y su potencial de impacto sistémico.

- **Posibles consecuencias**:
  - Compromiso y persistencia en VM que alojan datos.
  - Movimientos laterales hacia sistemas críticos y exfiltración masiva de información confidencial.
  - Interrupción de servicios esenciales (hospitales, plataformas bancarias, redes de energía) con impacto en continuidad operativa.
  - Pérdida de confianza pública y reputacional en instituciones afectadas. Posible sanción regulatoria por fallas en protección de datos.
  - Costos directos e indirectos por respuesta, remediación, multas y recuperación operacional.

- **Implicaciones en seguridad digital**:
  - Necesidad urgente de parches y gestión de vulnerabilidades con priorización por impacto critico.
  - Imperativo de segmentación de redes y aislamiento de entornos virtuales para limitar pivoting.
  - Fortalecimiento de detección (EDR/SIEM) orientada a ejecuciones desde rutas temporales, sockets inesperados y elevaciones rápidas.
  - Reforzamiento de controles de acceso y revisión de accesos iniciales que podrían permitir *exploits* locales.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Exploitation for Privilege Escalation	T1068	Los ciberdelincuentes explotan vulnerabilidades de software para elevar privilegios. CVE-2025-41244 es un ejemplo claro que permite que un actor con acceso local sin privilegios obtenga ejecución en contexto privilegiado (*root*) dentro de la VM.
Masquerading	T1036	Manipulación del nombre o la ubicación de un binario/servicio para hacerlo parecer legítimo. En este caso los atacantes modifican binarios con nombres de sistema (por ejemplo httpd en /tmp) para que la lógica de comprobación los trate como binarios válidos.
Valid Accounts	T1078	Uso o abuso de cuentas legítimas para acceder a sistemas. Dado que la vulnerabilidad requiere acceso local previo, el abuso de cuentas válidas (credenciales filtradas o cuentas con privilegios limitados) es una vía frecuente de entrada.
Create or Modify System Process	T1543	Creación o modificación de servicios y/o procesos del sistema para ejecutar payloads persistentemente. Tras el escalamiento, los ciberdelincuentes suelen intentar modificar servicios o unidades (systemd, servicios Windows) para mantener acceso y ejecutar código con privilegios elevados.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Update Software	M1051	Parchar y actualizar VMware Tools, VMware Aria y componentes relacionados es la medida más directa para eliminar la vulnerabilidad (CVE-2025-41244). Reduce la ventana de exposición frente a *exploits* confirmados y contrarresta la disponibilidad de PoC.
Execution Prevention	M1038	Los controles de ejecución dificultan que binarios colocados en /tmp o rutas temporales se ejecuten, mitigando la técnica de *masquerading* y la invocación privilegiada que explota la vulnerabilidad. Útil como medida compensatoria cuando no sea posible parchear de inmediato.
Restrict File and Directory Permissions	M1022	Restringir permisos de escritura y ejecución en directorios temporales y en rutas donde las herramientas de sistema buscan binarios, impide que usuarios no privilegiados coloquen ejecutables que luego sean invocados por procesos privilegiados.
Privileged Account Management	M1026	Limitar, auditar y controlar cuentas con privilegios reduce la probabilidad de que accesos válidos o abusados permitan alcanzar los estados necesarios para explotar la vulnerabilidad.

Soluciones y mitigaciones disponibles

- Para remediar la vulnerabilidad **CVE-2025-41244**, se recomienda aplicar de manera inmediata los parches publicados por VMware, actualizando a las versiones corregidas:
  - VMware Cloud Foundation (Cloud Foundation Operations 9.x.x.x): actualizar a 9.0.1.0.
  - VMware vSphere Foundation / VMware Tools (13.x.x.x en Windows y Linux): actualizar a 13.0.5.0.
  - VMware Aria Operations (8.x): actualizar a 8.18.5.
  - VMware Tools (13.x.x): actualizar a 13.0.5.
  - VMware Tools (12.x.x, 11.x.x): actualizar a 12.5.4.
  - VMware Cloud Foundation (Aria Operations 5.x, 4.x): aplicar KB92148.
  - VMware Telco Cloud Platform (Aria Operations 5.x, 4.x): actualizar a 8.18.5.
  - VMware Telco Cloud Infrastructure (Aria Operations 3.x, 2.x): actualizar a 8.18.5.

- Restringir los permisos de escritura y ejecución en directorios temporales como /tmp, evitando que usuarios sin privilegios puedan ubicar binarios que luego sean invocados con permisos elevados.
- Implementar controles de ejecución que permitan prevenir la ejecución de archivos no autorizados o que provengan de ubicaciones no seguras, utilizando listas blancas de aplicaciones o soluciones de seguridad de endpoint.
- Configurar la administración estricta de cuentas privilegiadas, reduciendo el número de usuarios con acceso de alto nivel, aplicando monitoreo de sesiones y reforzando el uso de autenticación multifactor.
- Monitorear de manera continua los registros y alertas del sistema en busca de intentos sospechosos de ejecución desde rutas no habituales o escaladas de privilegios, activando mecanismos de respuesta temprana.
- Documentar y probar un plan de respuesta ante incidentes que contemple la explotación de vulnerabilidades en VMware, garantizando tiempos rápidos de detección, contención y remediación.

Fuentes

Broadcom Support, 26/09/2025, 01/10/2025, VMware Security Advisory VMSA-2025-0023: CVE-2025-41244 and CVE-2025-41245, Fuente oficial del fabricante.
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

NVD - National Vulnerability Database, 26/09/2025, 01/10/2025, CVE-2025-41244 Detail, Fuente oficial gubernamental.
https://nvd.nist.gov/vuln/detail/CVE-2025-41244

The Hacker News, 29/09/2025, 01/10/2025, Urgent: China-linked Hackers Exploit New VMware Zero-Day Vulnerability, Medio de comunicación especializado en ciberseguridad.
https://thehackernews.com/2025/09/urgent-china-linked-hackers-exploit-new.html