Boletín informativo
Vulnerabilidad en VMware Aria Operations y VMware Tools

CSIRTSALUD-AV-20251104-12 **TLP: CLEAR**

Incidente ID:	0012
Fecha del reporte:	04/11/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en VMware Aria Operations y VMware Tools
Herramienta de detección	N/A
Activo involucrado:	VWware Aria Operations y VMware Tools
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema Digital sobre la vulnerabilidad crítica en VMware Tools y VMware Aria Operations, registrada como CVE-2025-41244, que está siendo explotada activamente en entornos reales.

Es de total importancia revisar esta vulnerabilidad en sus entornos debido a que es una vulnerabilidad con nivel de severidad Alta (CVSS 7.8) referente a una falla de escalada de privilegios local, adicionalmente está catalogada como una vulnerabilidad de 0-Day.

Descripción:

La vulnerabilidad permite a un atacante con privilegios limitados en una máquina virtual elevar sus permisos hasta nivel de administrador (root), logrando control total del sistema afectado. Esto facilita movimientos laterales, robo de datos o ejecución de código arbitrario en entornos virtualizados.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

El fallo está relacionado con el componente Service Discovery Management Pack (SDMP) de Aria Operations, utilizado en numerosas instalaciones corporativas de VMware.

Esta vulnerabilidad es de alta criticidad porque se ha confirmado que está siendo explotada activamente en ataques (zero-day). La agencia CISA de EE. UU. la ha añadido a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), lo que subraya la urgencia de su mitigación.

La vulnerabilidad toma como ruta de búsqueda no confiable (CWE-426) en el script get-versions.sh, que utiliza patrones de expresiones regulares muy amplios para localizar binarios de servicio. Un atacante podría colocar un binario malicioso en un directorio con permisos de escritura (por ejemplo, `/usr/ /tmp/httpdservices/bin`), que el proceso de detección de servicios de VMware ejecuta con privilegios elevados, otorgándole acceso completo de administrador.

Se puede detectar monitoreando procesos secundarios inusuales de vmtools o get-versions.sh, o inspeccionando archivos de script residuales en /tmp/VMware-SDMP-Scripts-{UUID}/.

La vulnerabilidad afecta tanto a la detección sin credenciales (mediante VMware Tools en máquinas virtuales invitadas) como a la detección heredada basada en credenciales (mediante VMware Aria Operations). Los investigadores han confirmado la misma falla en la biblioteca open-vm-tools incluida en la mayoría de las distribuciones de Linux.

Detalles de la vulnerabilidad:

Impacto: Estas vulnerabilidades podrían ser explotadas para ejecutar código malicioso de forma remota, robar información sensible o instalar malware.
La explotación de CVE-2025-41244 (CVSS 7.8) puede permitir:

- Escalada de privilegios desde un usuario limitado hasta administrador del sistema.
- Ejecución de código arbitrario en la máquina virtual comprometida.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Acceso no autorizado la otros sistemas o servicios dentro de la red.
- Exfiltración de información sensible.

Estado: Activamente Explotada (Zero-Day). Esta vulnerabilidad está siendo utilizada en ataques activos en el mundo real. Ha sido confirmada por agencias de ciberseguridad (como CISA) e incluida en el catálogo KEV (Known Exploited Vulnerabilities). Los parches de seguridad ya están disponibles.

Urgencia: La combinación de una severidad "Alta" (CVSS 7.8) y la explotación activa confirmada la convierte en una prioridad máxima. Las organizaciones deben parchear sus sistemas afectados de inmediato para prevenir un compromiso.

Vector de ataque: Un actor local malicioso con privilegios no administrativos que tenga acceso a una máquina virtual con VMware Tools instalado y administrado por Aria Operations con SDMP habilitado puede explotar esta vulnerabilidad para escalar privilegios a root en la misma máquina virtual.

Productos afectados:

- VMware Tools anteriores a la versión 13.0.5 (o 12.5.4 en la rama 12.x)
- VMware Aria Operations anteriores a la versión 8.18.5
- VMware Cloud Foundation Operations anteriores a la versión 9.0.1.0
- Open-vm-tools (la versión de código abierto para la mayoría de las distribuciones de Linux)

Afecta a entornos on-premise, nubes privadas y entornos híbridos que utilicen VMware Tools y Aria Operations.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Modo de explotación de la vulnerabilidad

El ataque se produce a través de un componente específico de las herramientas de VMware llamado Service Discovery Management Pack (SDMP).

El atacante debe tener acceso local y sin privilegios a una máquina virtual (VM) afectada, dicha VM debe tener VMware Tools instalado y estar siendo gestionada por VMware Aria Operations con la función SDMP habilitada.

La lógica del plugin SDMP ejecuta scripts de descubrimiento con privilegios elevados (root). La falla permite al atacante colocar un binario malicioso en una ubicación de escritura común (como /tmp), e l proceso de descubrimiento de servicios, al ejecutarse como root, ejecuta el binario malicioso del atacante, otorgándole control total sobre la máquina virtual.

Indicadores de Compromiso

- vmtoolsd – Proceso legítimo de VMware Tools que es abusado para cargar o ejecutar binarios maliciosos.
- /tmp/httpd – Ruta sospechosa usada por el atacante para alojar binarios maliciosos. El uso del directorio /tmp es típico en ataques para alojar o ejecutar código temporalmente como por ejemplo:

– /tmp
– /var/tmp
– /dev/shm

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones de mitigación:

Esta vulnerabilidad ha recibido una puntuación de 7.8 sobre 10 en la escala CVSS, por lo que es calificada como de gravedad alta. Para corregir este problema, es importante que se aplique lo antes posible las actualizaciones correspondientes. Esto ayudara a evitar ataques de este tipo, pero también a mantener un funcionamiento óptimo. En el caso de VMware Aria Operations, es necesario tener la versión 8.18.5, que es la que corrige el problema. En cuanto a VMware Tools, es necesario actualizar a la versión 13.0.5 y para Cloud Foundation Operations se necesita 9.0.1.0, o aplicar el parche KB92148 en versiones anteriores de Cloud Foundation. Puede acceder a toda la información y descargas desde las notas de lanzamiento oficiales para VMware Aria Operations 8.18.5 (VMSA-2025-0025) y para VMware Tools 13.0.5.

También se deben tener en cuenta las siguientes recomendaciones:

- Desactivar o limitar el uso del componente SDMP si no es necesario.
- Revisar y limitar los privilegios de los usuarios locales en las máquinas virtuales.
- Monitorizar procesos sospechosos relacionados con vmtoolsd y scripts en rutas temporales (por ejemplo, /tmp/VMware-SDMP-Scripts-{UUID}/).
- Aplicar segmentación de red y políticas de mínimos privilegios en contornos virtualizados.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/
- https://ciberseguridadegalicia.gal/es/ciberseguridad-al-dia/alertas/vulnerabilidad-0-day-en-vmware-tools-y-aria-operations-explotada-activamente#:~:text=La%20explotaci%C3%B3n%20de%20CVE%2D2025,servicios%20dentro%20de%20la%20red.
- https://socprime.com/es/blog/cve-2025-41244-zero-day-vulnerability/
- https://cwe.mitre.org/data/definitions/426.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-41244

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570