Boletín informativo
Vulnerabilidad en VMware Aria Operations (Broadcom)

CSIRTSALUD-AV-20260304-33 **TLP: CLEAR**

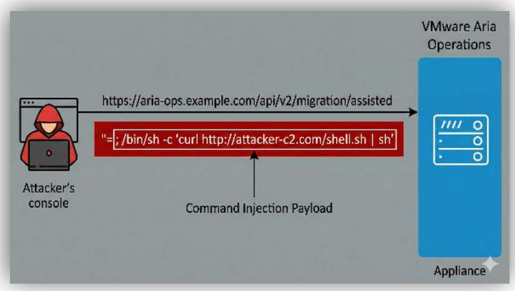
Incidente ID:	033
Fecha del reporte:	04/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en VMware Aria Operations
Herramienta de detección	N/A
Activo involucrado:	Appliance Virtual de VMware Aria Operations
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema sobre la existencia de tres vulnerabilidades críticas identificadas en VMware Aria Operations (VMSA-2026-0001), con énfasis en CVE-2026-22719, catalogada como activamente explotada en entornos reales por la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA).

Descripción:

VMware Aria Operations (anteriormente conocida como vRealize Operations) es una plataforma empresarial de monitoreo y gestión de infraestructuras que proporciona visibilidad sobre el rendimiento, la salud y el estado de servidores, redes y entornos de nube. Su posición central dentro de los ecosistemas de TI la convierte en un objetivo de alto valor para actores maliciosos.



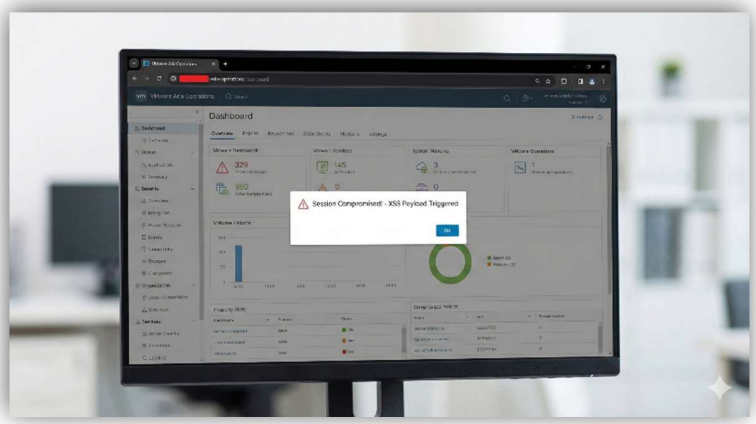
La vulnerabilidad **CVE-2026-22719** es un fallo de inyección de comandos (CWE-77) en VMware Aria Operations la cual reside en el flujo de trabajo de migración asistida por soporte (support-assisted product migration). El componente de migración no valida ni sanea

correctamente la entrada del usuario antes de incorporarla a comandos del sistema operativo. Caracteres especiales como punto y coma (;), barra vertical (|), ampersand (&) y comillas inversas (`) no son neutralizados, lo que permite a un atacante salir del contexto del comando legítimo e inyectar instrucciones arbitrarias en el sistema operativo subyacente.

Dado que el proceso de migración opera con privilegios elevados para realizar operaciones a nivel de sistema, una explotación exitosa puede otorgar al atacante control total sobre el appliance virtual afectado.

La explotación exitosa de esta falla tiene un impacto severo (Puntuación CVSSv3: 8.1):

- **Ejecución Remota de Código (RCE):** El atacante obtiene la capacidad de ejecutar código malicioso a nivel del sistema operativo.
- **Compromiso Total del Appliance:** Al tomar el control de la instancia de Aria Operations, el atacante puede acceder a configuraciones, credenciales de infraestructura y datos sensibles de monitorización.
- **Movimiento Lateral:** Al ser una herramienta central con amplia visibilidad, un atacante puede utilizar el servidor comprometido como cabeza de playa para moverse lateralmente hacia el entorno vSphere, vCenter u otras redes internas críticas.
- **Robo de datos sensibles:** Exfiltración de datos de rendimiento, configuraciones de red, credenciales de integraciones y secretos de API.
- **Despliegue de malware**: Instalación de backdoors, ransomware, cryptominers u otras herramientas de post-explotación.
- **Interrupción de operaciones**: Inhabilitación del monitoreo de infraestructura, impidiendo la detección temprana de incidentes adicionales.



CISA confirmó el 4 de marzo de 2026 que esta vulnerabilidad se encuentra siendo explotada activamente en entornos reales. Broadcom ha reconocido reportes de explotación aunque no puede confirmarlos de forma independiente.

Productos afectados:

La vulnerabilidad **CVE-2026-22719** (junto con las otras reportadas en el aviso VMSA-2026-0001) afecta directamente a **VMware Aria Operations**, así como a las grandes suites de infraestructura de VMware que lo incluyen como un componente integrado.

A continuación, te detallo los productos específicos, las versiones que son vulnerables y a qué versión exacta se debe actualizar para aplicar la corrección definitiva:

Producto	Versión Afectada	Versión Corregida
VMware Aria Operations	8.x — 8.18.5 y anteriores	8.18.6
VMware Cloud Foundation Operations	9.x — 9.0.1 y anteriores	9.0.2.0

Producto	Versión Afectada	Versión Corregida
VMware Cloud Foundation	5.x — 5.2.2 y anteriores	5.2.3
VMware Telco Cloud Platform	4.x / 5.x	5.2.3
VMware Telco Cloud Infrastructure	2.x / 3.x	5.2.3

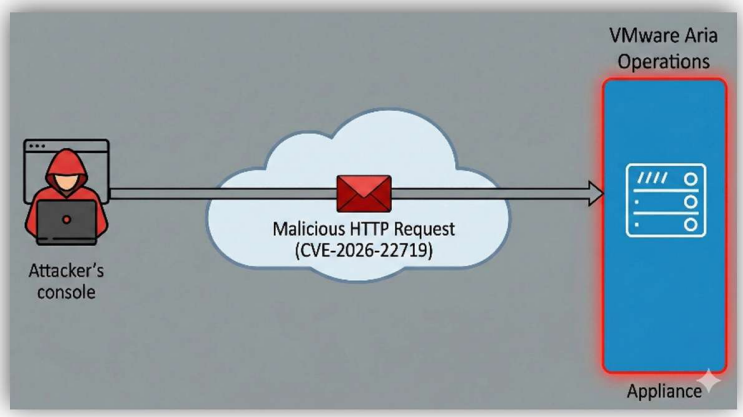
Modo de explotación y cadena de infección

Prerrequisitos del Ataque

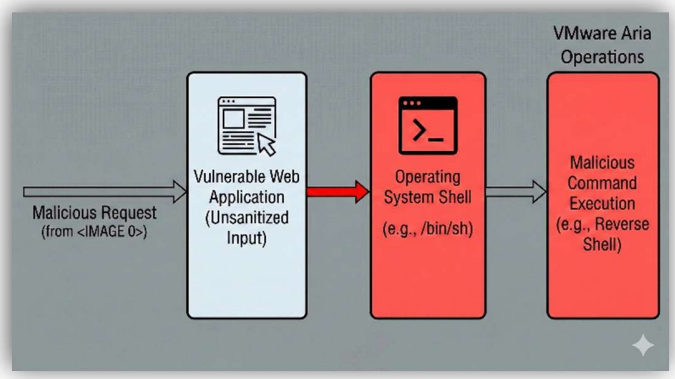
- Acceso de red al puerto de gestión de VMware Aria Operations (por defecto: HTTPS/443 o 8443).
- El proceso de migración asistida por soporte debe estar en progreso o puede ser iniciado por el atacante.
- No se requieren credenciales ni interacción del usuario (unauthenticated, no user interaction).

El proceso mediante el cual un atacante explota esta vulnerabilidad sigue estos pasos:

1. **Reconocimiento:** El atacante escanea la red en busca de instancias expuestas de VMware Aria Operations (versiones 8.x o 9.x).
2. **Identificación del Vector:** El atacante detecta que el endpoint de migración asistida por soporte está accesible.
3. **Inyección del Payload:** Se crea una solicitud HTTP/HTTPS maliciosa dirigida a la API responsable de la migración. Dentro de los parámetros de esta solicitud, el atacante concatena comandos del sistema operativo utilizando metacaracteres de shell (como ;comando_malicioso o |comando_malicioso).

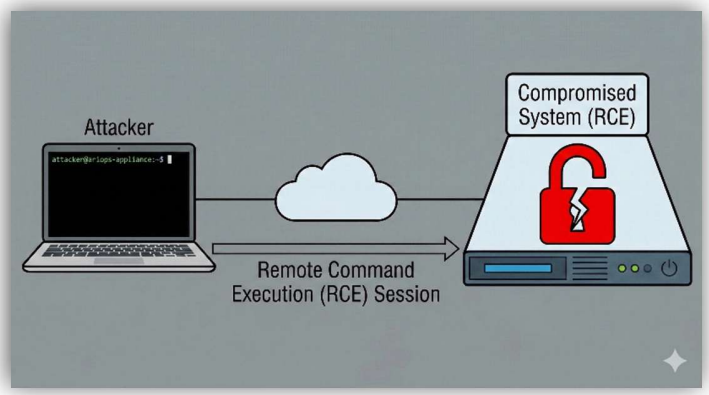


4. **Ejecución en el Backend:** La aplicación web de Aria Operations recibe la solicitud y la procesa sin realizar una validación o desinfección adecuada de las entradas (falta de sanitización). El parámetro manipulado se pasa directamente al intérprete de comandos del sistema operativo.



5. **Compromiso:** El sistema operativo ejecuta el comando inyectado con los altos privilegios del servicio de migración. Esto permite al atacante descargar herramientas

de hacking adicionales, establecer persistencia y obtener una consola interactiva remota.



Un actor sofisticado puede encadenar las tres vulnerabilidades para maximizar el impacto:

- **PASO 1 (CVE-22721):** Un actor con acceso limitado a vCenter aprovecha la escalada de privilegios para obtener rol de administrador en Aria Operations.
- **PASO 2 (CVE-22720):** Con privilegios de administrador, inyecta payloads JavaScript maliciosos en benchmarks personalizados. Cuando otro administrador visualiza el benchmark, su sesión es secuestrada.
- **PASO 3 (CVE-22719):** Usando la sesión robada o directamente sin autenticación, ejecuta la inyección de comandos durante el proceso de migración para obtener RCE completo.

EXPLICACIÓN DE CADA VULNERABILIDAD PARCHEADA (VMSA-2026-0001)

➢ 6.1. CVE-2026-22719 — Inyección de Comandos (CVSS 8.1)

Esta vulnerabilidad es la más peligrosa del advisory. Permite que un actor no autenticado con acceso de red a la interfaz de gestión ejecute comandos arbitrarios en el sistema operativo

del appliance. La falla se origina porque el componente de migración construye comandos del sistema concatenando entradas del usuario sin filtrar metacaracteres de shell. Los procesos de migración se ejecutan con privilegios elevados, lo que significa que los comandos inyectados heredan esos privilegios, potencialmente permitiendo control root sobre el sistema.

- **CVE-2026-22720 — Cross-Site Scripting Almacenado (CVSS 8.0)**

La plataforma permite almacenar datos suministrados por el usuario (en la creación de benchmarks) sin realizar la validación o codificación adecuada antes de mostrarlos en la interfaz web. Un atacante con permisos para crear benchmarks puede inyectar payloads JavaScript maliciosos que se almacenan permanentemente en la base de datos de la aplicación. Cuando un administrador de alto privilegio navega a la página que muestra el benchmark contaminado, el script se ejecuta en su navegador en el contexto de su sesión activa, permitiendo el robo de cookies de sesión, la realización de acciones administrativas no autorizadas (modificar configuraciones, crear usuarios, exportar datos) o redirigir al administrador a páginas de phishing.

CVE-2026-22721 — Escalada de Privilegios (CVSS 6.2)

Esta vulnerabilidad afecta la integración entre vCenter Server y Aria Operations. Un actor malicioso que ya posea privilegios dentro de vCenter puede aprovechar una validación inadecuada de permisos para obtener acceso administrativo completo en Aria Operations. Aunque requiere un nivel inicial de acceso (privilegios de vCenter), esta falla es particularmente relevante en escenarios de amenaza interna o cuando un atacante ya ha comprometido parcialmente el entorno de virtualización. El acceso administrativo a Aria Operations proporciona visibilidad sobre toda la infraestructura monitorizada y acceso a credenciales e integraciones críticas.

Relación con las Tácticas según MITRE ATT&CK

Las siguientes tácticas y técnicas del marco MITRE ATT&CK Enterprise son aplicables a la explotación de estas vulnerabilidades:

ID Técnica	Táctica	Descripción	CVE Relacionado
T1190	Acceso Inicial (Initial Access)	Exploit Public-Facing Application: Explotación de la interfaz de gestión de Aria Operations expuesta a la red mediante inyección de comandos sin autenticación.	CVE-2026-22719
T1059.004	Ejecución (Execution)	Command and Scripting Interpreter: Unix Shell. El payload inyectado se ejecuta en un intérprete de comandos Unix del appliance con privilegios elevados.	CVE-2026-22719
T1068	Escalada de Privilegios (Privilege Escalation)	Exploitation for Privilege Escalation: Aprovechamiento de la gestión inadecuada de privilegios entre vCenter y Aria Operations para obtener acceso administrativo.	CVE-2026-22721
T1078	Persistencia / Escalada (Persistence)	Valid Accounts: Post-explotación, el atacante puede crear cuentas válidas para mantener persistencia en el sistema.	CVE-2026-22719
T1185	Acceso a Credenciales (Credential Access)	Browser Session Hijacking (aplicado a contexto web app): El XSS almacenado permite capturar cookies de sesión administrativa activa.	CVE-2026-22720
T1059.007	Ejecución (Execution)	JavaScript: El payload XSS ejecuta código JavaScript malicioso en el navegador del administrador para realizar acciones en su nombre.	CVE-2026-22720

ID Técnica	Táctica	Descripción	CVE Relacionado
T1021.001	Movimiento Lateral (Lateral Movement)	Remote Services: Desde el appliance comprometido, el atacante puede usar credenciales o accesos obtenidos para moverse lateralmente a vCenter, ESXi y otros sistemas.	CVE-2026-22719
T1005	Recopilación (Collection)	Data from Local System: Extracción de archivos de configuración, credenciales de integraciones, certificados y datos de rendimiento almacenados en el appliance.	CVE-2026-22719
T1486	Impacto (Impact)	Data Encrypted for Impact (Ransomware): El acceso completo al appliance puede facilitar el despliegue de ransomware en la infraestructura de virtualización.	CVE-2026-22719
T1562.001	Evasión de Defensas (Defense Evasion)	Impair Defenses: Disable or Modify Tools. La desactivación del propio sistema de monitoreo (Aria Operations) impide la detección de actividades maliciosas posteriores.	CVE-2026-22719
T1040	Recopilación / Reconocimiento (Collection)	Network Sniffing: Desde una posición privilegiada en el appliance, el atacante puede capturar tráfico de gestión en la red de administración.	CVE-2026-22719

Indicadores de compromiso:

Dado que no existen aún IoC técnicos públicamente confirmados asociados a campañas específicas de explotación de CVE-2026-22719, los siguientes indicadores deben ser monitoreados activamente como señales de alarma:

Indicadores en Logs y Procesos

- Ejecución inusual de shells (/bin/sh, /bin/bash) iniciada por procesos de Aria Operations durante o después de ventanas de migración.
- Presencia de procesos no reconocidos con procesos padre relacionados a servicios de Aria Operations (vcops-*, cassandra, gemfire).
- Picos anómalos en CPU/memoria del appliance sin actividad de monitoreo legítima que los justifique.
- Árboles de procesos anormales: aparición de curl, wget, nc (netcat), python, perl lanzados desde servicios de Aria.
- Creación de archivos en rutas inusuales (/tmp, /var/tmp) con permisos de ejecución.
- Intentos de escritura en directorios de sistema o modificación de crontabs.

Indicadores de Red

- Tráfico de red saliente inesperado desde el appliance de Aria Operations hacia IPs externas o no catalogadas.
- Conexiones en puertos inusuales (especialmente salientes) desde el nodo de Aria Operations.
- Actividad de red hacia puertos de gestión de Aria Operations proveniente de IPs no autorizadas o fuera del rango de administración.
- Intentos de exfiltración de datos: transferencias HTTPS/HTTP de volumen inusual desde el appliance.
- Patrones de escaneo o reconocimiento hacia otros hosts internos desde la IP del appliance.

Indicadores de Aplicación

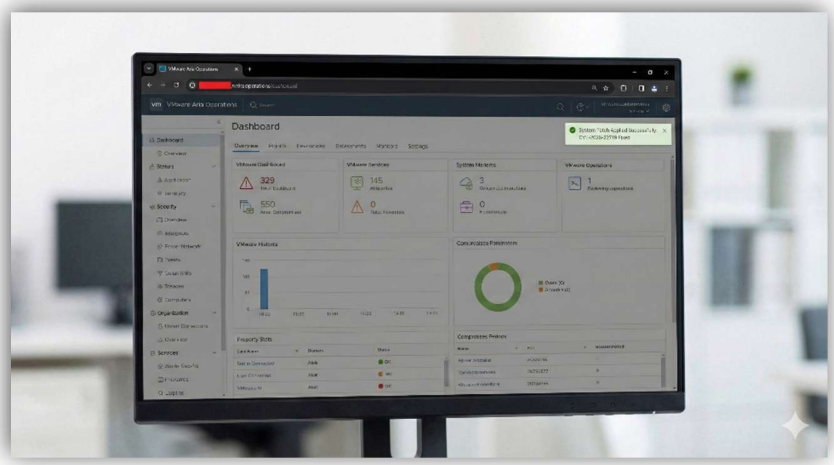
- Entradas de log que contengan caracteres de inyección: ;, |, &, $(), ``, %3B, %7C en campos de configuración de migración.

- Llamadas al sistema inesperadas en los logs de soporte o diagnóstico de Aria Operations.
- Creación de nuevos usuarios administrativos o cambios de contraseña no autorizados en la consola de Aria.
- Presencia de scripts personalizados de benchmark con payloads JavaScript sospechosos (indicativo de CVE-2026-22720).
- Accesos administrativos desde IPs o user-agents no habituales.
- Eventos de inicio de sesión exitosos seguidos inmediatamente de acciones de configuración masiva.

Recomendaciones de mitigación:

Broadcom ha lanzado parches para todas las versiones afectadas. Se recomienda aplicar los parches lo antes posible en todos los entornos afectados.

- Actualizar VMware Aria Operations 8.x a la versión 8.18.6 (resuelve CVE-2026-22719, CVE-2026-22720 y CVE-2026-22721).
- Actualizar VMware Cloud Foundation Operations 9.x a la versión 9.0.2.0.
- Actualizar VMware Cloud Foundation / Telco Cloud Platform versiones 4.x/5.x a la versión 5.2.3.
- Consultar la matriz de respuesta oficial en VMSA-2026-0001 (Broadcom Support Portal — SecurityAdvisory ID: 36947) para la versión específica de cada producto.
- Verificar la integridad de los parches antes de aplicarlos utilizando los hashes SHA proporcionados por Broadcom.



Mitigación Temporal (Si No Es Posible Parchear Inmediatamente)

- Descargar y ejecutar el script oficial aria-ops-rce-workaround.sh como usuario root en cada nodo del appliance de Aria Operations (disponible en KB430349). Este workaround aplica ÚNICAMENTE a CVE-2026-22719. Este script debe descargarse, copiarse a *todos* los nodos virtuales de Aria Operations vía SSH/SCP y ejecutarse.
- Posponer todos los procesos de migración asistida por soporte hasta que el parche esté aplicado.
- Restringir el acceso de red a la interfaz de gestión de Aria Operations mediante firewall, permitiendo solo rangos IP de administradores autorizados.
- Implementar segmentación de red (VLAN/microsegmentación) para aislar los servidores de gestión de Aria Operations de redes de usuarios generales.
- Deshabilitar temporalmente la funcionalidad de benchmarks personalizados si CVE-2026-22720 no puede ser parcheado.
- Revisar y auditar los privilegios de las cuentas de vCenter que tienen acceso a Aria Operations (relacionado con CVE-2026-22721).

Fuentes:

- https://www.bleepingcomputer.com/news/security/cisa-flags-vmware-aria-operations-rce-flaw-as-exploited-in-attacks/
- https://thehackernews.com/2026/03/cisa-adds-actively-exploited-vmware.html
- https://gbhackers.com/vmware-aria-flaws/
- https://humeit.com/blog/vmsa-2026-0001-evaluating-risk-in-vmware-aria-operations
- https://diamatix.com/vmware-aria-operations-rce-vmsa-2026-0001/
- https://attack.mitre.org/matrices/enterprise/
- https://www.cisa.gov/news-events/alerts/2026/03/03/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947
- https://knowledge.broadcom.com/external/article/430349
- https://techdocs.broadcom.com/us/en/vmware-cis/aria/aria-operations/8-18/vmware-aria-operations-8186-release-notes.html

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.