Nro. Alerta:	AL-2025-005	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	07-feb-2025	**Vulnerabilidad en VMware Aria**	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Información

Nivel de riesgo: Alto

II. ALERTA

El proveedor de tecnología empresarial VMware Broadcom envió el 30 de enero de 2025 parches para al menos cinco defectos de seguridad en sus productos Aria Operations y Aria Operations for Logs, advirtiendo que los piratas informáticos podrían explotar estos problemas para obtener acceso de administrador.

Figura 1.- *Ilustración asociada a VMware Aria.* ***Fuente: The Hacker News***

III. INTRODUCCIÓN

Broadcom ha lanzado actualizaciones de seguridad para corregir cinco fallas de seguridad que afectan a VMware Aria Operations y Aria Operations for Logs, advirtiendo a los clientes que los atacantes podrían explotarlas para obtener acceso elevado u obtener información confidencial.

La empresa advirtió que la vulnerabilidad CVE-2025-22218 (puntuación de gravedad CVSS 8,5/10) afecta al producto empresarial Aria Operations for Logs. VMware manifestó

que los usuarios con permisos de "*Solo administrador de visualización*" podrían acceder a las credenciales de un producto VMware integrado.

El segundo problema de divulgación de información, que afecta a Aria Operations, es que permite que un usuario con privilegios no administrativos recupere credenciales para un complemento saliente si se conoce una identificación de credencial de servicio válida.

La compañía también detectó varios problemas de gravedad moderada que permiten ataques de secuencias de comandos entre sitios (XSS) almacenados, donde usuarios que no son administradores pueden inyectar un script malicioso que se ejecuta como administrador, lo que potencialmente permite acciones no autorizadas.

VMware también corrigió una vulnerabilidad de control de acceso rota en Aria Operations for Logs que puede ser explotada por un usuario no administrador con acceso de red a la API para ejecutar operaciones como administrador.

IV. VECTOR DE ATAQUE.

- **CVE-2025-22218** (puntuación CVSS: 8,5): un actor malintencionado con permisos de administrador de solo lectura podría leer las credenciales de un producto VMware integrado con VMware Aria Operations for Logs
- **CVE-2025-22219** (puntuación CVSS: 6,8): un actor malintencionado con privilegios no administrativos puede inyectar un script malicioso que puede provocar operaciones arbitrarias como usuario administrador a través de un ataque de secuencias de comandos entre sitios (XSS) almacenado
- **CVE-2025-22220** (puntuación CVSS: 4,3): un actor malintencionado con privilegios no administrativos y acceso de red a la API de Aria Operations for Logs puede realizar determinadas operaciones en el contexto de un usuario administrador.
- **CVE-2025-22221** (puntuación CVSS: 5,2): un actor malintencionado con privilegios de administrador en VMware Aria Operations for Logs podría inyectar un script malicioso que podría ejecutarse en el navegador de una víctima al realizar una acción de eliminación en la configuración del agente.
- **CVE-2025-22222** (puntuación CVSS: 7,7): un usuario malintencionado con privilegios no administrativos puede aprovechar esta vulnerabilidad para recuperar credenciales para un complemento saliente si se conoce una ID de credencial de servicio válida.

V. IMPACTO

Las vulnerabilidades en los productos de VMware a las siguientes versiones:

- VMware Aria Operations
- VMware Aria Operations for Logs
- Operaciones de VMware Aria para registros
- Operaciones de VMware Aria
- Fundación VMware Cloud

VI. RECOMENDACIONES:

La empresa advirtió que no existen soluciones alternativas previas a la aplicación de parches para estas vulnerabilidades, lo que significa que es necesario aplicar parches para mitigar los riesgos. La empresa publicó correcciones en Aria Operations for Logs 8.18.3 y Aria Operations 8.18.3.

VII. DESCARGO DE RESPONSABILIDAD.

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS.

- https://thehackernews.com/2025/01/broadcom-patches-vmware-aria-flaws.html
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25329
- https://securityaffairs.com/173677/security/vmware-aria-operations-flaws.html