Nro. Alerta:	AL-2026-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-jun-2026	Vulnerabilidades XSS en VMware podrían permitir acciones administrativas no autorizadas (CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724)	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación de vulnerabilidades XSS en plataformas VMware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidades XSS en VMware podrían permitir acciones administrativas no autorizadas (CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724) - Figura referencial

Broadcom ha revelado tres vulnerabilidades de tipo Cross-Site Scripting (XSS) Stored, identificadas como CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724, estas permitirían a un atacante autenticado inyectar código JavaScript malicioso en elementos configurables de la plataforma como políticas, vistas o widgets de texto en una interfaz web para comprometer entornos administrativos. Las fallas afectan a VMware Cloud Foundation Operations y a varios productos relacionados, incluidos VMware Aria Operations, VMware Cloud Foundation, VMware vSphere Foundation y VMware Telco Cloud Platform.

Nro. Alerta:	AL-2026-033	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-jun-2026	Vulnerabilidades XSS en VMware podrían permitir acciones administrativas no autorizadas (CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724)	Pág.: **2** of **5**

III. INTRODUCCIÓN

VMware Cloud Foundation es una plataforma de infraestructura de nube privada e híbrida que integra virtualización, almacenamiento, redes, seguridad, gestión y automatización en una única solución para construir un Centro de Datos Definido por Software (SDDC). Permite desplegar y operar infraestructura de forma consistente en centros de datos propios, edge y de nubes compatible.

Sus componentes principales son:

- VMware vSphere (incluye vCenter Server) para la Virtualización de servidores y máquinas virtuales.
- VMware vSAN, se emplea para el almacenamiento definido por software.
- VMware NSX, se utiliza para redes virtuales y microsegmentación.
- VMware SDDC Manager en la gestión y automatización del entorno.

Componentes de gestión y operaciones:

- VCF Operations, utilizado para el monitoreo, análisis, capacidad, optimización, cumplimiento y operaciones.
- VCF Automation, para automatización y orquestación de servicios e infraestructura en la nube mediante flujos de trabajo y catálogos de autoservicio.

Cross-Site Scripting (XSS) es una falla de seguridad web que permite a un atacante inyectar código JavaScript malicioso en una aplicación para que sea ejecutado por el navegador de otros usuarios.

XSS Stored, es un tipo de XSS en donde el payload malicioso, se almacena permanentemente en la aplicación (base de datos, widgets, vistas, perfiles, comentarios, tickets, etc.).

IV. VECTOR DE ATAQUE

Las vulnerabilidades CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724 tienen un vector de ataque de tipo RED y un nivel de severidad de 8.0

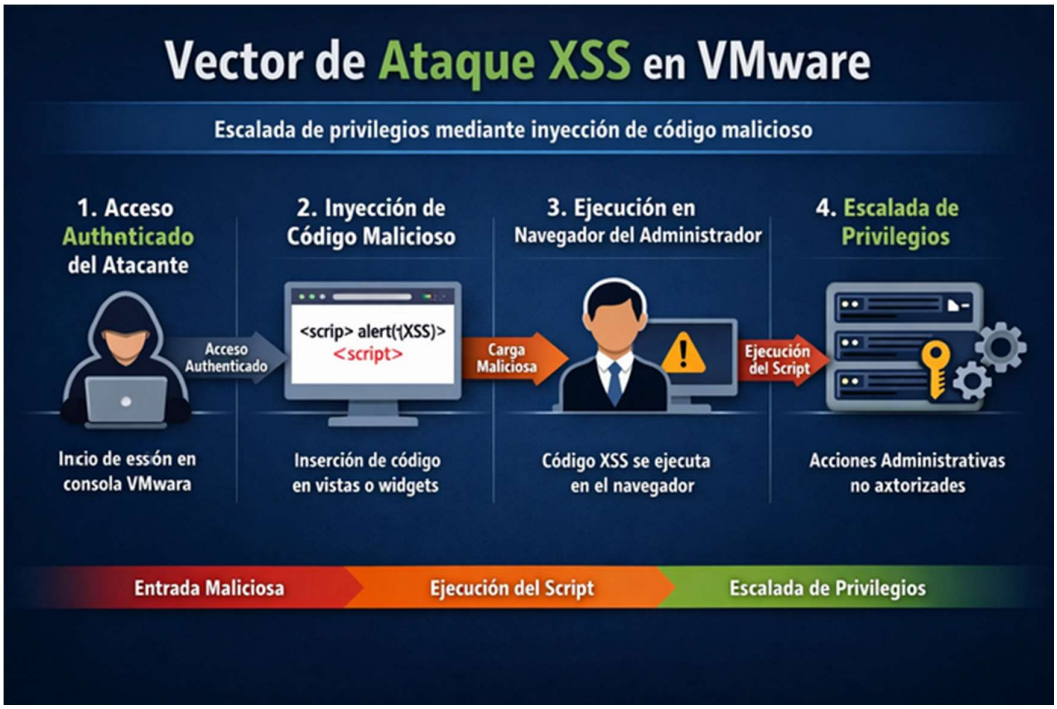

Figura 2.- Vector de Ataque- Vulnerabilidades XSS en VMware podrían permitir acciones administrativas no autorizadas (CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724)

Las vulnerabilidades residen en los componentes de VCF Operations y se debe a una validación insuficiente de las entradas, ya sea en widgets, vistas o formularios, así como a una codificación inadecuada de las salidas, lo que permite que datos proporcionados por un usuario sean interpretados por el navegador como código ejecutable en lugar de texto plano.

Como resultado de estas deficiencias en el tratamiento de las entradas y salidas, un atacante puede almacenar payloads maliciosos de JavaScript dentro de la plataforma (XSS Stored), para posteriormente, cuando un usuario con privilegios, incluidos los administradores, accedan al contenido afectado y los scripts inyectados se ejecuten en el contexto de la sesión de su navegador, permitiendo potencialmente el robo de información sensible, la ejecución de acciones en nombre del usuario o la alteración del contenido mostrado por la aplicación.

Dado que VCF Operations suele integrarse con otros componentes del ecosistema de VMware, como vCenter y los flujos de trabajo de automatización en la nube, su explotación podría tener efectos en cadena en entornos híbridos y multinube.

Los atacantes que aprovechan estas fallas también pueden combinarlas con otras vulnerabilidades o configuraciones erróneas para escalar privilegios o mantener la persistencia.

V. IMPACTO

Productos	Componentes	Versiones afectadas	CVE	Versión fija
VMware Cloud Foundation VMware vSphere Foundation	VMware Cloud Foundation Operations	9.1.x.x	CVE-2026-41722, CVE-2026-41723	9.1.0.0
VMware Cloud Foundation VMware vSphere Foundation	VMware Cloud Foundation Operations	9.0.x.x	CVE-2026-41722, CVE-2026-41723	9.0.2.0 EP2
VMware Aria Operations	N/A	8.x	CVE-2026-41722, CVE-2026-41723	8.18.6
VMware Aria Operations	N/A	8.x	CVE-2026-41722, CVE-2026-41723, CVE-2026-41724	8.18.7
VMware Cloud Foundation	VMware Aria Operations	5.x	CVE-2026-41722, CVE-2026-41723, CVE-2026-41724	8.18.7
VMware Telco Cloud Platform	VMware Aria Operations	5.x	CVE-2026-41722, CVE-2026-41723, CVE-2026-41724	KB443138

Tabla 1.- Productos afectados - Vulnerabilidades XSS en VMware podrían permitir acciones administrativas no autorizadas (CVE-2026-41722, CVE-2026-41723 y CVE-2026-41724)

VI. INDICADORES DE COMPROMISO

- Creación o modificación no autorizada de Policies, Views o Text Widgets.
- Presencia de código HTML o JavaScript embebido en widgets o vistas.
- Solicitudes HTTP/HTTPS hacia dominios externos al cargar dashboards administrativos.
- Actividades administrativas realizadas desde sesiones o direcciones IP inusuales.
- Eventos de auditoría que evidencien la modificación de componentes visuales seguida de acciones administrativas no autorizadas.
- Posible robo o reutilización de sesiones de administradores mediante ejecución de código JavaScript persistente.

VII. RECOMENDACIONES:

- Auditar roles administrativos periódicamente y eliminar accesos innecesarios o cuentas inactivas.
- Actualizar VMware Cloud Foundation Operations y Aria Operations, junto con los demás productos afectados, a las versiones corregidas publicadas por Broadcom.
- Sensibilizar a usuarios privilegiados sobre los riesgos de ataques XSS y la importancia de validar cambios realizados en la plataforma.
- Revisar objetos configurados recientemente en busca de código HTML o JavaScript no autorizado que pueda indicar intentos de explotación.
- Limitar la creación de políticas, vistas y widgets únicamente a usuarios estrictamente autorizados.
- Integrar registros con SIEM para detectar actividades anómalas asociadas a escalamiento de privilegios o modificaciones no autorizadas.
- Implementar autenticación multifactor (MFA) para todos los usuarios con acceso a las consolas de administración.
- Restringir acceso a plataformas VMware desde redes administrativas seguras y estaciones de trabajo controladas.
- Asignar permisos mínimos necesarios para cada función, reduciendo el riesgo de abuso por parte de usuarios comprometidos.

VIII. 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.

IX. REFERENCIAS:

BROADCOM (2026). VMSA-2026-0004: VMware Cloud Foundation Operations updates address multiple vulnerabilities. *https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37513*

TELCONET CSIRT (2026). VMware Cloud Foundation Operations Faces Multiple Stored XSS Vulnerabilities. *https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidades-*