

Alert Bulletin

Bulletin N.:

Publication Date: 19/06/2025

Subject: Alerta 2025-51- Vulnerabilidades XSS en VMware NSX

Traffic Light Protocol (TLP): Amber



Producto(s) afectado(s):

Las versiones de NSX afectadas incluyen 4.2.x, 4.2.1.x, 4.1.x y 4.0.x

- NSX 4.2.x < 4.2.2.1
- NSX 4.2.1.x < 4.2.1.4
- NSX 4.1.x y 4.0.x < 4.1.2.6

VMware Cloud Foundation:

- 5.2.x
- 5.1.x, 5.0.x
- 4.5 x

Infraestructura de nube de VMware Telco

- 3.x, 2.x
- 5.x, 4.x, 3.x

Descripción

Se ha publicado varias fallas de seguridad de tipos Stored XSS que afectan al VMware NSX, las cuales exponen a los usuarios a ataques de secuencias de comandos entre sitios (XSS) almacenadas. Estas fallas, identificadas como CVE-2025-22243, CVE-2025-22244 y CVE-2025-22245, afectan a diversos productos de VMware, como VMware NSX, VMware Cloud Foundation y VMware Telco Cloud Platform.

- CVE-2025-22243 XSS en la interfaz de NSX Manager (CVSS 7.5 Gravedad importante).
 Un atacante con privilegios para modificar la configuración de red podría inyectar scripts maliciosos en la interfaz de NSX Manager.
- CVE-2025-22244 XSS en el firewall de puerta de enlace (CVSS 6.9 Gravedad moderada).

 Esta vulnerabilidad permite la inyección de código a través de la página de respuesta del filtro de URL dentro de la interfaz del firewall de puerta de enlace. Un agente malicioso con acceso para crear o modificar

beaconlab.us



la página de respuesta del filtro de URL podría inyectar código malicioso que se ejecuta cuando otro usuario intenta acceder al sitio web filtrado.

• CVE-2025-22245 - XSS en el puerto del enrutador (CVSS 5.9 - Gravedad moderada).

El XSS almacenado en la configuración del puerto del enrutador podría permitir que se activen ataques cuando otros usuarios inspeccionan la configuración del enrutador. *Un atacante con privilegios para crear o modificar puertos del enrutador podría inyectar código malicioso que se ejecuta cuando otro usuario intenta acceder al puerto del enrutador*.

Para ver el boletín de seguridad completo publicado por el proveedor, puede redirigirse al siguiente enlace:

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25738

Solución:

El proveedor a dispuesto parches de seguridad que solucionan las vulnerabilidades abordadas:

- NSX 4.2.x ⋈4.2.2.1
- NSX 4.2.1.x ⊠4.2.1.4
- NSX 4.1.x y 4.0.x ⊠4.1.2.6

Para los usuarios de VMware Cloud Foundation (v5.0–5.2), Broadcom recomienda la actualización asíncrona a NSX a la versión 4.2.2.1 o 4.1.2.6 siguiendo las instrucciones de:

https://knowledge.broadcom.com/external/article?legacyld=88287

Los usuarios de Telco Cloud pueden consultar el siguiente enlace para más información sobre la actualización:

https://knowledge.broadcom.com/external/article/396986

Información adicional:

- https://securityonline.info/multiple-stored-xss-vulnerabilities-discovered-in-vmware-nsx-patch-now/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25738

