VMware NSX – Multiple Stored XSS Vulnerabilities

TL;DR

VMware NSX has three newly patched XSS flaws (CVE-2025-22243, CVE-2025-22244, CVE-2025-22245) in its Manager UI, firewall, and router components. CVSS score range from 5.9 to 7.5.

If an attacker with access injects malicious code, it will execute when viewed by another user. There are no workarounds, and it is best to patch immediately.

Overview

Three stored cross-site scripting (XSS) vulnerabilities (CVE-2025-22243, CVE-2025-22244, CVE-2025-22245) were found in VMware NSX, impacting the Manager UI, gateway firewall, and router port components. These flaws, caused by improper input validation, can allow privileged users to inject persistent scripts that execute when viewed by others. This could lead to session hijacking, administrative access, or data compromise.

Affected Products

- VMware NSX (versions 4.0.x – 4.2.x)
- VMware Cloud Foundation (versions 5.0.x – 5.2.x)
- VMware Telco Cloud Infrastructure (versions 2.x – 3.x)
- VMware Telco Cloud Platform (versions 3.x – 5.x)

Vulnerability Breakdown

- **CVE-2025-22243** – NSX Manager UI (CVSS 7.5)
  A threat actor with permissions to create or alter network settings could inject persistent scripts into the Manager UI. When another user views the modified settings, the injected code may execute in their browser, leading to session hijacking or other unintended actions.

- **CVE-2025-22244** – Gateway Firewall (CVSS 6.9)
  Attackers with access to modify URL filtering response pages could inject scripts that trigger when users access filtered sites. This could lead to script execution in the user's browser context without their knowledge.

- **CVE-2025-22245** – Router Port (CVSS 5.9)
  Privileged users could inject malicious scripts into router port configurations. When other users access these ports, the scripts could execute, opening the door to further compromise.

Stored XSS in admin tools gives attackers a foothold in environments. If an attacker already has access, this makes privilege abuse or lateral movement easier. Although these vulnerabilities have not been exploited, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Apply the appropriate patch version immediately.
- Restrict NSX administrative access to only those who need it.
- Review logs for unusual changes to network settings or router configurations.
- If async patching is required, follow Broadcom's KB articles for Cloud Foundation and Telco Cloud systems.

TTPs to Watch

Privilege Escalation

- Exploitation for Client Execution [T1203] – The attacker may inject malicious scripts through exposed NSX interfaces requiring UI access.

Credential Access

- Input Capture [T1056] – Scripts may be used to steal session tokens or admin credentials if viewed by another user.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These vulnerabilities affect sectors relying on NSX for network virtualization and segmentation. Industries at risk include:

- Cloud Hosting Providers
- Telecom
- Healthcare
- Large Enterprises managing virtualized environments
- Finance

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Support Content Notification - Support Portal - Broadcom support portal
NVD - CVE-2025-22245

NVD - CVE-2025-22244
NVD - CVE-2025-22243