مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-VMware vCenter & NSX Products
Tracking #:432317761
Date:30-09-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Broadcom has released security updates to address multiple vulnerabilities in VMware vCenter Server and VMware NSX products. These vulnerabilities impact VMware Cloud Foundation, NSX-T, VMware vCenter, and Telco Cloud components.

TECHNICAL DETAILS:

Broadcom has released security updates to address multiple vulnerabilities in VMware vCenter Server and VMware NSX products. These vulnerabilities impact VMware Cloud Foundation, NSX-T, VMware vCenter, and Telco Cloud components.

Successful exploitation could lead to credential exposure, account compromise, and potential lateral movement within enterprise environments. Administrators are strongly advised to patch affected systems immediately

Vulnerability Details
1. CVE-2025-41250 – SMTP Header Injection (vCenter)
   - Severity: Important | CVSS 8.5
   - Description: Exploitable by authenticated, non-admin users with scheduled task creation rights. Could manipulate notification emails.
   - Workaround: None available.
   - Fix: Apply patches (vCenter 9.0.1.0, 8.0 U3g, 7.0 U3w, VCF 5.2.2, async patches for older versions, KB updates for VCF & Telco Cloud).
2. CVE-2025-41251 – Weak Password Recovery (NSX)
   - Severity: Important | CVSS 8.1
   - Description: Allows unauthenticated attackers to exploit the password recovery function to enumerate usernames.
   - Workaround: None available.
   - Fix: Upgrade to fixed versions (NSX 9.0.1.0, 4.2.2.2 / 4.2.3.1, 4.1.2.7, NSX-T 3.2.4.3, or KB updates for VCF & Telco Cloud).
3. CVE-2025-41252 – Username Enumeration (NSX)
   - Severity: Important | CVSS 7.5
   - Description: Username enumeration vulnerability that increases brute-force risks.
   - Workaround: None available.
   - Fix: Same patch set as CVE-2025-41251.

Impacted Products
The following products and versions are confirmed vulnerable:
   - VMware vCenter Server (7.x, 8.x, 9.x)
   - VMware NSX (versions 9.x, 4.2.x, 4.1.x, 4.0.x)
   - NSX-T (3.x)
   - VMware Cloud Foundation (versions 4.x, 5.x)
   - VMware Telco Cloud Platform & Infrastructure (versions 2.x – 5.x)

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RECOMMENDATIONS:

- **Patch Immediately** – Apply vendor-provided patches and KB updates as per the response matrix.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERNCES:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36150