مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - VMware

Tracking #:432317291

Date:21-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that VMware has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in VMware Cloud Foundation, ESXi, vCenter Server, Workstation, and Fusion. These vulnerabilities could allow attackers to gain unauthorized access, execute arbitrary commands, cause denial-of-service (DoS) conditions, or perform cross-site scripting (XSS) attacks.

Vulnerabilities Details:

VMware Cloud Foundation Updates Address Multiple Vulnerabilities

- **CVE-2025-41229: Directory Traversal Vulnerability**
  - **Description:** Allows a malicious actor with network access to port 443 on VMware Cloud Foundation to access certain internal services.
  - **Severity:** Important (CVSSv3: 8.2)
- **CVE-2025-41230: Information Disclosure Vulnerability**
  - **Description:** Allows a malicious actor with network access to port 443 on VMware Cloud Foundation to gain access to sensitive information.
  - **Severity:** Important (CVSSv3: 7.5)
- **CVE-2025-41231: Missing Authorisation Vulnerability**
  - **Description:** Allows a malicious actor with access to the VMware Cloud Foundation appliance to perform unauthorized actions and access limited sensitive information.
  - **Severity:** Important (CVSSv3: 7.3)

Affected Versions and Fixes:

- VMware Cloud Foundation 5.x: Update to 5.2.1.2
- VMware Cloud Foundation 4.5.x: Refer to KB398008

VMware ESXi, vCenter Server, Workstation, and Fusion Updates Address Multiple Vulnerabilities:

- **CVE-2025-41225: VMware vCenter Server Authenticated Command-Execution Vulnerability**
  - **Description:** An authenticated malicious actor with privileges to create or modify alarms and run script action can run arbitrary commands on the vCenter Server.
  - **Severity:** Important (CVSSv3: 8.8)
- **CVE-2025-41226: Guest Operations Denial-of-Service Vulnerability**
  - **Description:** A malicious actor with guest operation privileges on a VM, authenticated through vCenter Server or ESXi, can create a denial-of-service condition of guest VMs with VMware Tools running and guest operations enabled.
  - **Severity:** Moderate (CVSSv3: 6.8)
- **CVE-2025-41227: Denial-of-Service Vulnerability**
  - **Description:** A malicious actor with non-administrative privileges within a guest operating system can exhaust memory of the host process leading to a denial-of-service condition.
  - **Severity:** Moderate (CVSSv3: 5.5)
- **CVE-2025-41228: VMware ESXi and vCenter Server Reflected Cross-Site Scripting (XSS) Vulnerability**

- **Description:** A malicious actor with network access to the login page of certain ESXi host or vCenter Server URL paths can steal cookies or redirect to malicious websites.
- **Severity:** Moderate (CVSSv3: 4.3)

Affected Versions and Fixes:

- **vCenter Server:**
  - 8.0: Update to 8.0 U3e
  - 7.0: Update to 7.0 U3v
- **VMware ESXi:**
  - 8.0: Update to ESXi80U3se-24659227
  - 7.0: Update to ESXi70U3sv-24723868
- **VMware Cloud Foundation (vCenter):**
  - 5.x: Async patch to 8.0 U3e (refer to KB88287)
  - 4.5.x: Async patch to 7.0 U3v (refer to KB88287)
- **VMware Cloud Foundation (ESXi):**
  - 5.x: Async patch to ESXi80U3se-24659227 (refer to KB88287)
  - 4.5.x: Async patch to ESXi70U3sv-24723868 (refer to KB88287)
- **VMware Telco Cloud Platform (ESXi):**
  - 5.x, 4.x, 3.x, 2.x: Update to ESXi80U3se-24659227
- **VMware Telco Cloud Infrastructure (ESXi):**
  - 3.x: Update to ESXi80U3se-24659227
  - 2.x: Update to ESXi70U3sv-24723868
- **VMware Telco Cloud Platform (vCenter):**
  - 5.x, 4.x, 3.x, 2.x: Update to 8.0 U3e
- **VMware Telco Cloud Infrastructure (vCenter):**
  - 3.x: Update to 8.0 U3e
  - 2.x: Update to 7.0 U3v
- **VMware Workstation:**
  - 17.x: Update to 17.6.3
- **VMware Fusion:**
  - 13.x: Update to 13.6.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by VMware.

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.

REFERENCES:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25717
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25733