مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in VMware Fusion

Tracking #:432318962

Date:14-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a privilege escalation vulnerability in VMware Fusion. This vulnerability could allow a low-privileged local user to gain elevated (root) privileges on affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-41702
- **Severity:** Important | CVSS 7.8
- VMware Fusion contains a Time-of-Check to Time-of-Use (TOCTOU) vulnerability in a SETUID binary operation. The flaw arises due to a race condition between validation and execution, which may allow an attacker to manipulate privileged operations.

Impact

A local authenticated attacker with non-administrative privileges may exploit this vulnerability to escalate privileges to root on the affected system, potentially gaining full control over the host.

Affected Products

- VMware Fusion 25H2 (Any platform)

Fixed Versions / Mitigations

- VMware Fusion 26H1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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/0/37454