مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Authentication Bypass Vulnerability in VMware Tools

Tracking #:432317012

Date:26-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed VMware released a security advisory (VMSA-2025-0005) addressing a high-severity authentication bypass vulnerability (CVE-2025-22230) in VMware Tools for Windows.

TECHNICAL DETAILS:

VMware released a security advisory (VMSA-2025-0005) addressing a high-severity authentication bypass vulnerability (CVE-2025-22230) in VMware Tools for Windows.

Vulnerability Overview

- **CVE ID**: CVE-2025-22230
- **Affected Product**: VMware Tools for Windows (versions 11.x.x and 12.x.x prior to 12.5.1)
- **Vulnerability Type**: Authentication Bypass due to Improper Access Control
- **CVSS v3 Base Score**: 7.8 (High)
- **Attack Vector**: Local
- The vulnerability stems from improper access control mechanisms within VMware Tools for Windows. An attacker with non-administrative privileges on a Windows guest VM can exploit this flaw to bypass authentication and perform certain high-privilege operations within the affected virtual machine
- **Fixed Versions**: VMware Tools for Windows 12.5.1

RECOMMENDATIONS:

- Users should update VMware Tools to the fixed version on all Windows guest VMs as soon as possible.
- Implement a proactive patch management policy to ensure that VMware products are up to date.

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/0/25518