



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Vulnerability in VMware Workstation and Fusion Products**

Tracking #:432315659

Date:28-02-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Vulnerability in VMware Workstation and Fusion products that could be exploited to obtain sensitive information from affected systems.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-22251**
- CVSS Score 5.9 Medium
- An out-of-bounds read vulnerability exists in the USB CCID (chip card interface device) of VMware Workstation and Fusion. This vulnerability could allow a malicious actor with local administrative privileges on a virtual machine to potentially disclose sensitive information.
- A successful exploit of this vulnerability could allow an attacker to read sensitive information from the vulnerable system. This information may include memory contents or other internal data.

### Affected Products:

- VMware Workstation Pro / Player (Workstation)
- VMware Fusion

Product	Affected Version	Running On	Fixed Version
VMware Workstation	17.x	Any	17.5.1
VMware Fusion	13.x	OS X	13.5.1

## 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://www.vmware.com/security/advisories/VMSA-2024-0005.html>