



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates- Critical Vulnerabilities VMware Products**

Tracking #:432315679

Date:06-03-2024

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 observed that VMware released security updates to address multiple vulnerabilities in its products.

## TECHNICAL DETAILS:

On March 5, 2024, VMware released security patches to address vulnerabilities in its ESXi, Workstation, Fusion, and Cloud Foundation products. These vulnerabilities could allow attackers with local administrative privileges on a virtual machine to escape the sandbox and potentially execute code on the underlying host system.

### Vulnerabilities Details:

- **CVE-2024-22252 (Critical)**: Use-after-free vulnerability in the XHCI USB controller. (CVSSv3 score: 9.3 for Workstation/Fusion, CVSSv3 score 8.4 for ESXi)
- **CVE-2024-22253 (Critical)**: Use-after-free vulnerability in the UHCI USB controller. (CVSSv3 score: 9.3 for Workstation/Fusion, CVSSv3 score 8.4 for ESXi)
- **CVE-2024-22254 (High)**: Out-of-bounds write vulnerability in ESXi. (CVSSv3 score: 7.9)
- **CVE-2024-22255 (High)**: Information disclosure vulnerability in the UHCI USB controller. (CVSSv3 score: 7.1)

### Affected Products:

- VMware ESXi
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)
- VMware Cloud Foundation (Cloud Foundation)

### Mitigations:

Product	Version	Running On	Fixed Versions	Workarounds
ESXi	8	Any	ESXi80U2sb-23305545	KB96682
ESXi	8.0 [2]	Any	ESXi80U1d-23299997	KB96682
ESXi	7	Any	ESXi70U3p-23307199	KB96682
Workstation	17.x	Any	17.5.1	KB96682
Fusion	13.x	MacOS	13.5.1	KB96682
Cloud Foundation (ESXi)	5.x/4.x	Any	KB88287	KB96682

- A patch available with extended support for ESXi 6.7 (6.7U3u), 6.5 (6.5U3v), and VCF 3.x.
- Additional patches available for ESXi 8.0 U1. If you do not plan to update your environment to ESXi 8.0 Update 2b (build # 23305546), use 8.0 Update 1d to update your ESXi hosts of version 8.0 Update 1c (build # 22088125) and earlier for these security fixes. The supported update path from 8.0 Update 1d is to ESXi 8.0 Update 2b or later. For more information, see the [Product Interoperability Matrix](#).



## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2024-0006.html>