



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Multiple Vulnerabilities in VMware products**

Tracking #:432315632

Date:21-02-2024

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 multiple vulnerabilities in VMware products that could be exploited to gain unauthorized access to affected systems.

## TECHNICAL DETAILS:

### 1.CVE-2024-22245-Arbitrary Authentication Relay Vulnerability in Deprecated EAP Browser Plugin

- CVSSv3 Score: **9.6 Critical**
- An Arbitrary Authentication Relay vulnerability exists in the VMware Enhanced Authentication Plug-in (EAP). This vulnerability allows a malicious actor to trick a target domain user with EAP installed in their web browser into requesting and relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs).

### 2.CVE-2024-22250-Session Hijack Vulnerability in Deprecated EAP Browser Plugin

- CVSSv3 Score: **7.8 High**
- A session hijacking vulnerability exists in the VMware Enhanced Authentication Plug-in (EAP). This vulnerability allows a threat actor with unprivileged local access to a Windows operating system to hijack a privileged EAP session initiated by a privileged domain user on the same system.

### 3.CVE-2024-22235-VMware Aria Operations Local Privilege Escalation vulnerability.

- CVSSv3 Score **6.7 Medium**
- VMware Aria Operations contains a local privilege escalation vulnerability. An attacker with administrative access to the system can exploit this vulnerability to escalate their privileges to "root".

Product	Version	Fixed Version
VMware Enhanced Authentication Plug-in (EAP)	Any	<u>KB96442</u>
VMware Aria Operations	8.x	8.16
VMware Cloud Foundation (VMware Aria Operations)	4.x, 5.x	<u>KB92148</u>

## 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:

1. <https://www.vmware.com/security/advisories.html>