مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates- VMware Avi Load Balancer Multiple Vulnerabilities

Tracking #:432315849

Date:14-05-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in VMware Avi Load Balancer. These vulnerabilities could be exploited by malicious actors to gain unauthorized access to systems and sensitive information.

## TECHNICAL DETAILS:

**Vulnerabilities Details:**

- **CVE-2024-22264:** Privilege Escalation Vulnerability
  - Severity: Important (CVSSv3 Base Score: 7.2)
  - An attacker with administrative privileges on VMware Avi Load Balancer can exploit this vulnerability to gain root access on the underlying host system. This allows them to create, modify, execute, and delete files with full system privileges.
- **CVE-2024-22266:** Information Disclosure Vulnerability
  - Severity: Moderate (CVSSv3 Base Score: 6.5)
  - VMware Avi Load Balancer stores cloud connection credentials in plain text within system logs. An attacker with access to these logs can view the credentials and potentially use them to compromise cloud resources.

**Affected Versions:**

- VMware Avi Load Balancer versions 22.1.x prior to 22.1.6
- VMware Avi Load Balancer versions 30.x.x prior to 30.2.1

**Fixed Versions:**

- VMware Avi Load Balancer version 22.1.6
- VMware Avi Load Balancer version 30.2.1

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version 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/0/24219