

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



SQL Injection Vulnerability in VMware Avi Load Balancer
Tracking #:432316800
Date:29-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed VMware has identified a high-severity unauthenticated blind SQL Injection vulnerability (CVE-2025-22217) in its Avi Load Balancer product.

TECHNICAL DETAILS:

VMware has identified a high-severity unauthenticated blind SQL Injection vulnerability (CVE-2025-22217) in its Avi Load Balancer product. This vulnerability, with a CVSSv3 base score of 8.6, allows malicious actors with network access to execute specially crafted SQL queries, potentially gaining unauthorized access to sensitive database information.

Vulnerability Overview:

- CVE Identifier: CVE-2025-22217
- Severity: High (CVSSv3 Score: 8.6)
- Impacted Product: VMware Avi Load Balancer
- Vulnerability Type: Unauthenticated Blind SQL Injection

Affected Versions:

The following versions of VMware Avi Load Balancer are impacted:

- 30.1.1
- 30.1.2
- 30.2.1
- 30.2.2

Resolution:

- For versions 30.1.1 and 30.1.2, upgrade to version 30.1.2-2p2
- For version 30.2.1, upgrade to version 30.2.1-2p5
- For version 30.2.2, upgrade to version 30.2.2-2p2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the security patches provided by VMware as soon as possible.

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/0/25346>