مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SQL Injection Vulnerability in Zoho Analytics On-Premise
Tracking #:432318020
Date:17-11-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical unauthenticated SQL Injection (SQLi) vulnerability has been identified in Analytics Plus On-Premise installations.

TECHNICAL DETAILS:

A critical unauthenticated SQL Injection (SQLi) vulnerability has been identified in Analytics Plus On-Premise installations prior to Build 6171. Tracked as CVE-2025-8324, this flaw allows remote attackers to execute arbitrary SQL queries without authentication, potentially leading to unauthorized exposure of sensitive user information. Successful exploitation could result in account compromise, data leakage, or full database access.

Critical Vulnerability Details:
- CVE-2025-8324
- CVSS v3:Base Score: 9.8
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Severity: Critical
- Unauthenticated SQL Injection due to the improper filter configuration
- Affected Versions: Zoho Analytics On-Premise builds below 6170
- Fixed Version- Zoho Analytics On-Premise Build 6171

RECOMMENDATIONS:

- Users are strongly advised to upgrade to the latest fixed version immediately.

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.zoho.com/analytics/onpremise/CVE-2025-8324.html