



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Vulnerability in Apache Solr**

Tracking #:432316404

Date:17-10-2024

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 a critical vulnerability, CVE-2024-45216, has been discovered in Apache Solr, specifically affecting instances utilizing the PKIAuthenticationPlugin.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-45216**-CVSS Score 9.8 **Critical**
- This vulnerability allows for authentication bypass through the use of manipulated API URLs, potentially exposing sensitive data and operations to unauthorized users.

### Affected Products:

- Apache Solr versions 5.3.0 before 8.11.4
- Apache Solr versions 9.0.0 before 9.7.0

### Fixed Versions:

- Apache Solr to version 9.7.0 or 8.11.4

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://solr.apache.org/security.html#cve-2024-45216-apache-solr-authentication-bypass-possible-using-a-fake-url-path-ending>