مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Solr

Tracking #:432319057

Date:03-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Solr affects deployments that enabled Basic Authentication using the bin/solr auth enable utility. The issue introduces template accounts with hardcoded credentials that could allow attackers to gain unauthorized administrative access to affected Solr clusters.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-44825**
- **Severity:** Critical
- A hardcoded credentials vulnerability exists in Apache Solr's Basic Authentication setup utility (bin/solr auth enable). When used to bootstrap authentication, the tool silently creates additional template users with publicly known credentials alongside user-defined accounts. An attacker could exploit these credentials to gain full administrative access to vulnerable Solr clusters.
- Successful exploitation could allow unauthorized administrative access, configuration changes, unauthorized data access, service disruption, and compromise of cluster integrity.

Affected Versions

- Apache Solr (org.apache.solr:solr-core) 9.4.0 through 9.10.1
- Apache Solr (org.apache.solr:solr-core) 10.0.0

Not affected:
* Clusters where bin/solr auth enable was not used to bootstrap BasicAuth
* Clusters where template users have been assigned strong passwords after bootstrap

Fixed Versions / Mitigations
Immediate Workarounds:

- Remove template accounts (superadmin, admin, search, index) from the security.json or change their passwords

Fixed Versions:

- Apache Solr 9.11.0 or later (upon release)
- Apache Solr 10.1.0 or later (upon release)

RECOMMENDATIONS:

- Identify systems using Basic Authentication configured via bin/solr auth enable
- Audit authentication configurations and remove unnecessary accounts
- Restrict administrative interfaces from public exposure
- Monitor authentication logs for unauthorized access attempts
- Prioritize upgrades once fixed versions become available
- Implement periodic credential and access reviews across Solr deployments

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.tenable.com/cve/CVE-2026-44825