مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Apache Kyuubi

Tracking #:432318212

Date:06-01-2026

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 INTELLGIENCE 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 high-severity vulnerability in Apache Kyuubi that could allow unauthorized users to access the server's local file system, weakening the platform's data security and isolation mechanisms.

TECHNICAL DETAILS:

A high-severity security vulnerability has been identified in Apache Kyuubi, a distributed gateway designed to provide secure, serverless SQL access to large-scale data lakes. The vulnerability could allow unauthorized users to access the server's local file system, weakening Kyuubi's data security and isolation mechanisms.

Vulnerability Details

- **CVE-2025-66518**
- **CVSS v3.1 Score:** 8.8 (High)
- The issue stems from missing path normalization in how the Kyuubi Server validates file paths. Apache Kyuubi uses the configuration parameter kyuubi.session.local.dir.allow.list to restrict client access to approved local directories. Due to insufficient path sanitization, these restrictions can be bypassed.
- Any client with access to the Apache Kyuubi Server through supported frontend protocols may exploit this flaw to access local files outside the configured allow-list.

Impact

Successful exploitation may allow an attacker to:

- Access unauthorized local directories
- Read sensitive configuration or system files
- Bypass administrative access controls
- Compromise multi-tenant isolation guarantees

Affected Versions

- Apache Kyuubi (org.apache.kyuubi:kyuubi-server) 1.6.0 through <=1.10.2

Fixed Version

- Apache Kyuubi version 1.10.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache Kyuubi.

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://nvd.nist.gov/vuln/detail/CVE-2025-66518