مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Denial-of-Service Vulnerability in Apache Karaf Decanter

Tracking #:432318312

Date:26-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Apache Karaf Decanter that could allow an unauthenticated remote attacker to cause a denial-of-service (DoS) condition by exploiting unsafe deserialization in a specific component.

TECHNICAL DETAILS:

A significant security vulnerability has been identified in Apache Karaf Decanter, a monitoring solution used to collect and dispatch logs and system metrics in enterprise environments. The vulnerability, tracked as CVE-2026-24656, could allow an unauthenticated remote attacker to cause a Denial of Service (DoS) condition by exploiting unsafe deserialization in a specific Decanter component.

Vulnerability Details

- **CVE-2026-24656**
- The issue affects the Decanter log socket collector, which listens for incoming log events on TCP port 4560. This port is exposed without authentication by default. When configured to accept "allowed classes," the collector's validation can be bypassed, allowing attackers to send crafted serialized objects. This results in deserialization of untrusted data, causing the Decanter service to crash and disrupting log collection and monitoring operations.
- The vulnerability does not allow code execution but can significantly impact availability by disabling visibility into system events.

Affected Products

- Apache Karaf Decanter versions prior to 2.12.0

Fixed Versions

- Apache Karaf Decanter 2.12.0 or later

RECOMMENDATIONS:

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

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://seclists.org/oss-sec/2026/q1/112