مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Apache SeaTunnel

Tracking #:432317074

Date:14-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Apache SeaTunnel that could potentially be exploited to gain unauthorized access and control over affected systems.

TECHNICAL DETAILS:

A security vulnerability, **CVE-2025-32896**, has been disclosed in Apache SeaTunnel, a widely used distributed data integration platform. This vulnerability allows unauthenticated attackers to exploit a legacy REST API endpoint to perform arbitrary file reads and execute remote code via unsafe deserialization. Given SeaTunnel's adoption by large-scale organizations for massive data synchronization, this flaw poses a significant risk to enterprise environments.

Vulnerability Details:

- The vulnerability resides in the legacy REST API endpoint: /hazelcast/rest/maps/submit-job
- Attackers can exploit this endpoint by submitting malicious jobs using RESTful API v1, injecting parameters into a MySQL connection URL to achieve the following:
  - **Arbitrary File Read**: Access sensitive files on the server's filesystem (e.g., configuration files, credentials).
  - **Remote Code Execution (RCE)**: Trigger unsafe Java object deserialization to execute malicious payloads.
- Successful exploitation can lead to:
  - **Data Exposure**: Unauthorized access to sensitive data stored on the server.
  - **System Compromise**: Full server control via RCE, enabling attackers to deploy malware or exfiltrate data.
  - **Operational Disruption**: Potential service outages or data corruption due to malicious activity

Affected Versions:

- Apache SeaTunnel versions: **2.3.1 through 2.3.10**

Mitigation:

- upgrade to version 2.3.11, and enable restful api-v2 & open https two-way authentication.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Apache SeaTunnel.

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://lists.apache.org/thread/s2dw28t4p0q6t3k0qoqnm18t6pt04pyt